Projektive Geometrie

von

Heinz Lüneburg

Aus dem Nachlass des Autors herausgegeben
von Theo Grundhöfer und Karl Strambach

Vorwort der Herausgeber

Heinz Lüneburg ist am 19. Januar 2009 plötzlich verstorben. Über sein Buchprojekt „Projektive Geometrie“ war auf seiner homepage zu lesen:

> Dieses Buch, im WS 1967/68 begonnen, sollte mein erstes Buch werden. Dass es dies nicht wurde, lag an meinem Wechsel nach Kaiserslautern. Vier Kapitel waren damals mit meiner Reiseschreibmaschine aufgeschrieben. Hier hatten wir aber nur Studenten im ersten Semester, so dass ich keine Vorlesungen über den Gegenstand halten konnte, wobei jedoch die „Einführung in die Algebra“ von den Vorarbeiten für jenes Buch profitierte. Es blieb also liegen. Es blieb liegen, bis ich die Vorlesungen über Fibonacci begann. Diese Vorlesungen waren einstündig. Die eine Stunde bedurfte jedoch einer Woche an Vorbereitung. Also griff ich in die Konserve und hielt neben der Vorlesung über Fibonacci noch eine vierstündige Vorlesung über projektive Geometrie. ... Das Buch liegt also jetzt da, 525 Seiten im ehemaligen B.I.-Format, und es fehlt noch ein Kapitel. Wann ich dieses schreiben kann, weiß ich nicht. Vielleicht publiziere ich es ohne das fehlende Kapitel über orthogonale Gruppen.

Leider enthält der Nachlass von Heinz Lüneburg nur einen rudimentären Anfang dieses Kapitels über orthogonale Gruppen, nämlich die Konstruktion von Cliffordalgebren, und keine Spuren von einem weiteren geplanten Kapitel „Anwendungen“. Mit der freundlichen Zustimmung von Frau Karin Lüneburg machen wir die im Nachlass vorhandenen Kapitel der Öffentlichkeit zugänglich.

Die Projektive Geometrie von Heinz Lüneburg spiegelt die zeitlichen Veränderungen wider, welchen auch die Mathematik unterworfen ist. Das Buch beginnt mit einem verbandstheoretischen Aufbau, gemäß der grundlagentheoretischen Perspektive der 1960er Jahre. In den Kapiteln IIII und V wird die Lüneburgsche Sicht auf die endliche Geometrie und auf Polaritäten deutlich. Die Kapitel VI und VII zeigen, dass Heinz Lüneburg sich für die Burausche Welt der synthetischen algebraischen Geometrie erwärmen konnte und zu dieser Theorie moderne, einsichtige Beweise geliefert hat.

Ein Vortrag von Karl Strambach zur Erinnerung an Heinz Lüneburg ist als Anhang beigefügt.

Würzburg, im Juni 2011 — Theo Grundhöfer und Karl Strambach

Inhaltsverzeichnis

I.

Die Grundlagen und ein bisschen mehr

Projektive Geometrien sind zunächst Inzidenzstrukturen, bestehend aus Punkten und Geraden mit gewissen Eigenschaften. Wie sich herausstellt, verbirgt sich dahinter eine reiche Struktur, nämlich der Verband der Unterräume dieser Geometrien. In diesem Kapitel wird es nun vor allem darum gehen, diese Verbände vom verbandstheoretischen Standpunkt aus in den Griff zu bekommen, soweit dies ohne Verwendung von Methoden der linearen Algebra, die hinter all dem steckt, ohne Zwang möglich ist. Insbesondere werden wir den Basissatz beweisen und zeigen, dass eine projektive Geometrie, deren Dimension nicht gerade 2 ist, stets desarguessch ist. Dies impliziert wiederum, dass ein projektiver Verband, dessen Dimension mindestens 3 ist, dem Unterraumverband eines geeigneten Vektorraums isomorph ist. Da die Dimension dieses Vektorraumes um 1 größer ist als die Dimension der zugehörigen Geometrie, werden wir das Wort Dimension nur informell benutzen und stattdessen vom Rang einer projektiven Geometrie und vom Rang eines Vektorraumes reden.

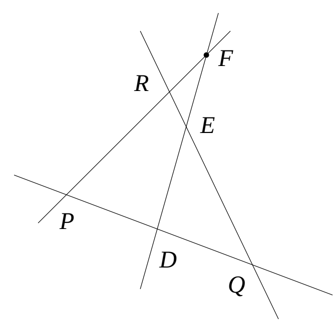
Nicht zu den Grundlagen dessen, was weiter folgt, gehören die Ausführungen über vollständig reduzible Ringe. Sie sind hier aufgenommen, weil man an ihnen demonstrieren kann, wie nützlich der Begriff des projektiven Verbandes ist. Hinzu kommt, dass die projektive Deutung der einschlägigen Sätze Einsichten vermittelt, die man in Algebrabüchern vergeblich sucht.

1. Projektive Räume

Es sei Π eine Menge, deren Elemente wir *Punkte*, und Γ eine Menge, deren Elemente wir *Geraden* nennen. Ferner sei I eine Teilmenge des cartesischen Produktes $\Pi \times \Gamma$ von Π und Γ. Ist $(P, G) \in \mathrm{I}$, so sagen wir, dass P mit G *inzidiere*, andernfalls, dass P und G *nicht inzidierten*. Statt P inzidiere mit G werden wir auch andere Redewendungen wie P *liege auf* G oder G *gehe durch* P oder P *sei enthalten in* G oder ähnliche verwenden. Statt $(P, G) \in \mathrm{I}$ bzw. $(P, G) \notin \mathrm{I}$ werden wir meist $P \mathrel{\mathrm{I}} G$ bzw. $P \not\mathrel{\mathrm{I}} G$ schreiben. Das Tripel $(\Pi, \Gamma, \mathrm{I})$ heißt *Inzidenzstruktur*.

Es sei $(\Pi, \Gamma, \mathrm{I})$ eine Inzidenzstruktur und $\Phi \subseteq \Pi$. Die Punkte von Φ heißen *kollinear*, falls es ein $G \in \Gamma$ gibt mit $X \mathrel{\mathrm{I}} G$ für alle $X \in \Phi$. Sind P und Q zwei verschiedene kollineare Punkte und gibt es nur eine Gerade durch P und Q, so bezeichnen wir diese mit $P + Q$. Diese Bezeichnung soll an die Addition von Unterräumen eines Vektorraumes erinnern, da die so bezeichnete Verknüpfung am Ende nichts anderes als diese sein wird.

Aus den unübersehbar vielen Inzidenzstrukturen sondern wir die projektiven Geometrien durch die folgende Definition aus. Die Inzidenzstruktur $\Sigma := (\Pi, \Gamma, \mathrm{I})$ heißt *projektive Geometrie* oder auch *projektiver Raum*, falls Σ den folgenden Bedingungen genügt.
(P1) Sind P und Q zwei verschiedene Punkte von Σ, so gibt es genau eine Gerade G von Σ mit P, $Q \mathrel{\mathrm{I}} G$.
(P2) Sind P, Q und R drei nicht kollineare Punkte von Σ und sind D und E zwei weitere, verschiedene Punkte mit $D \mathrel{\mathrm{I}} P + Q$ und $E \mathrel{\mathrm{I}} Q + R$, so gibt es einen Punkte F mit $F \mathrel{\mathrm{I}} R + P$ und $F \mathrel{\mathrm{I}} D + E$.
(P3) Jede Gerade von Σ trägt wenigstens zwei Punkte.



Veblen-Young Axiom

Axiom (P2) wird häufig *Veblen-Young Axiom* genannt. Man kann es salopp auch so formulieren: Trifft eine Gerade zwei Seiten eines Dreiecks in verschiedenen Punkten, so trifft sie auch die dritte Seite.

Beispiele von projektiven Geometrien sind leicht zu verschaffen. Die einfachsten Beispiele sind die folgenden: Ist M eine Menge und bezeichnet $P_2(M)$ die Menge der Teilmengen mit genau zwei Elementen von M, so ist $(M, P_2(M), \in)$ eine projektive Geometrie. So banal diese Beispiele auch erscheinen mögen, so werden sie uns doch später beim Beweise des Satzes von Wielandt über die Automorphismengruppe der alternierenden Gruppe ein sehr nützliches Werkzeug sein.

Projektive Geometrien, deren Geraden mehr als zwei Punkte tragen, erhält man folgendermaßen: Es sei V ein Vektorraum über dem Körper K. Bezeichnet man mit $\mathrm{UR}_i(V)$ die Menge der Unterräume des Ranges i von V, so ist $(\mathrm{UR}_1(V), \mathrm{UR}_2(V), \subseteq)$ eine projektive Geometrie. (Der Leser erinnere sich, dass Rang hier das ist, was anderenorts meist Dimension genannt wird.) Dies zu beweisen, sei dem Leser als Übungsaufgabe überlassen. Ein Tipp sei jedoch gegeben. Sind pK und qK zwei verschiedene Punkte, so sind pK, qK und $(p+q)K$ drei verschieden Punkte auf der Geraden $pK + qK$.

Es seien $(\Pi, \Gamma, \mathrm{I})$ und $(\Pi', \Gamma', \mathrm{I}')$ zwei Inzidenzstrukturen. Ferner sei σ eine Bijektion von Π auf Π' und τ eine solche von Γ auf Γ'. Das Paar (σ, τ) heißt *Isomorphismus* von $(\Pi, \Gamma, \mathrm{I})$ auf $(\Pi', \Gamma', \mathrm{I}')$, wenn für alle $P \in \Pi$ und alle $G \in \Gamma$ genau dann $P \mathrel{\mathrm{I}} G$ gilt, wenn $P^\sigma \mathrel{\mathrm{I}'} G^\tau$ ist. Gibt es einen solchen Isomorphismus,

so nennen wir die beiden Inzidenzstrukturen *isomorph*. Isomorphismen einer Inzidenzstruktur auf sich heißen *Automorphismen* oder *Kollineationen*.

1.1. Satz. *Es sei* $\Sigma := (\Pi, \Gamma, \mathrm{I})$ *ein projektiver Raum. Ist* $G \in \Gamma$, *so setzen wir* $G^\tau := \{P \mid P \in \Pi, P \,\mathrm{I}\, G\}$. *Dann ist* (id_Π, τ) *ein Isomorphismus von* Σ *auf* $(\Pi, \Gamma^\tau, \in)$.

Beweis. Das Einzige, was zu beweisen ist, ist die Injektivität von τ. Diese folgt aber unmittelbar aus der Tatsache, dass jede Gerade mindestens zwei Punkte trägt und zwei verschiedene Punkte nur mit einer Geraden inzidieren.

Dieser Satz zeigt, dass man die Geraden eines projektiven Raumes mit den Mengen der jeweils auf ihnen liegenden Punkte identifizieren kann. Dies ist immer wieder einmal bequem und wird, meist ohne es explizit zu sagen, dann auch getan.

Es sei $\Sigma := (\Pi, \Gamma, \mathrm{I})$ ein projektiver Raum und $U \subseteq \Pi$. Die Menge U heißt *Unterraum* von Σ, falls mit zwei verschiedenen Punkten stets auch ihre ganze Verbindungsgerade in U liegt. (Hier haben wir zum ersten Male Geraden mit Punktmengen identifiziert.) Beispiele von Unterräumen sind die leere Menge $\emptyset$, die Mengen, die nur aus einem Punkt bestehen, die Geraden und Π. Wir bezeichnen die Menge aller Unterräume von Σ mit $L(\Sigma)$. Sind X, $Y \in L(\Sigma)$ und ist X in Y enthalten, so bezeichnen wir diesen Sachverhalt mit $X \leq Y$. Wir benutzen in diesem Falle also das Zeichen $\leq$ anstelle von $\subseteq$. Die Relation $\leq$ ist *reflexiv*, *antisymmetrisch* und *transitiv*, dh. sie ist eine *Teilordnung* auf $L(\Sigma)$. Diese Teilordnung gilt es nun zu studieren.

Damit der Leser ein Gefühl dafür bekomme, was Unterräume sind, beweise er das Folgende: Es sei V ein K-Vektorraum. Ferner sei X eine Teilmenge von $\mathrm{UR}_1(V)$. Genau dann ist X ein Teilraum von $(\mathrm{UR}_1(V), \mathrm{UR}_2(V), \subseteq)$, wenn es einen Teilraum W von V gibt mit $X = \mathrm{UR}_1(W)$.

Ist M eine Menge, so ist $L(M, P_2(M), \in)$ nichts Anderes als die Potenzmenge von M.

Es ist im Weiteren bequem, die Unterräume, die nur aus einem Punkt bestehen, mit diesem Punkt zu identifizieren, so dass sich also die Inzidenz des Punktes P mit der Geraden G durch $P \leq G$ beschreiben läßt. Damit sind der Begriff des Punktes und der Begriff der Geraden unter den Begriff des Unterraumes subsumiert, so dass die Ausnahmestellung dieser Objekte beseitigt ist.

Es sei weiterhin Σ eine projektive Geometrie. Ist $M \subseteq L(\Sigma)$, so ist, wie unmittelbar aus der Definition des Unterraumes folgt, auch $\bigcap_{X \in M} X \in L(\Sigma)$. Wie üblich definiert man daher den von M *aufgespannten Unterraum* $\sum_{X \in M} X$ von Σ als den Schnitt über alle Unterräume Y von Σ, für die $X \leq Y$ für alle $X \in M$ gilt. Es gilt dann die folgende banale, aber nützliche Aussage.

1.2. Satz. *Es sei* Σ *eine projektive Geometrie. Es sei ferner* $M \subseteq L(\Sigma)$ *und* $Y \in L(\Sigma)$. *Dann gilt: Ist* $Y \leq X$ *für alle* $X \in M$, *so ist* $Y \leq \bigcap_{X \in M} X$. *Ist* $X \leq Y$ *für alle* $X \in M$, *so ist* $\sum_{X \in M} X \leq Y$.

Dieser Satz besagt, dass $\bigcap_{X \in M} X$ der größte, in allen $X \in M$ enthaltene Unterraum von Σ ist, während $\sum_{X \in M} X$ der kleinste, alle $X \in M$ umfassende Unterraum von Σ ist.

Die Definition des Operators $\sum$, der im Übrigen das ist, was man einen *Hüllenoperator* nennt, ist zwar elegant, man hätte aber auch gerne eine interne Beschreibung des von einer Menge von Unterräumen aufgespannten Unterraums. Diese Beschreibung wird in Kürze gegeben werden. Dazu definieren wir zunächst eine binäre Verknüpfung $\odot$ auf der Potenzmenge der Punktmenge Π eines projektiven Raumes.

(1) Es ist $S \odot \emptyset = \emptyset \odot S = S$ für alle $S \subseteq \Pi$.
(2) Ist S eine einelementige Teilmenge von Π, so setzen wir $S \odot S = S$.
(3) Sind S und T Teilmengen von Π und gibt es zwei verschiedene Punkte P und Q mit $P \in S$ und $Q \in T$, so sei $S \odot T$ die Menge der Punkte, die auf den Geraden liegen, die zwei verschiedene Punkte A und B mit $A \in S$ und $\mathrm{B} \in T$ verbinden.

Die wesentlichen Eigenschaften dieser Operation sind im folgenden Satz aufgelistet.

1.3. Satz. *Es sei $\Sigma := (\Pi, \Gamma, \mathrm{I})$ eine projektive Geometrie. Sind S, T und U drei Teilmengen von Π, so gilt:*
(a) *Ist $S \subseteq T$, so ist $S \odot U \subseteq \mathrm{T} \odot U$. Insbesondere ist $S \subseteq S \odot S$.*
(b) *Es ist $S \odot T = T \odot S$.*
(c) *Ist $R \in L(\Sigma)$ und gilt $S, T \subseteq R$, so ist $S \odot T \subseteq R$.*
(d) *Es ist $(S \odot T) \odot U = S \odot (T \odot U)$.*
(e) *Genau dann gilt $S \odot S = S$, wenn $S \in L(\Sigma)$ ist.*
(f) *Sind $S, T \in L(\Sigma)$, so ist $S \odot T = S + T$.*

Beweis. (a) Die erste Aussage von (a) folgt unmittelbar aus der Definition von $\odot$. Wendet man dies nun statt auf S, T und U auf $\emptyset$, S und S an, so folgt

$$S = \emptyset \odot S \subseteq S \odot S.$$

(b) und (c) folgen unmittelbar aus der Definition von $\odot$ und der definierenden Eigenschaft von Unterräumen mit zwei Punkten ihre Verbindungsgerade zu enthalten.

Um (d) zu beweisen, nehmen wir zunächst an, dass alle drei Mengen nur aus einem Punkt bestehen, so dass wir sie gemäß unserer Konvention mit diesen Punkten identifizieren. Liegen S, T und U auf der Geraden G, so folgt mit (c), dass $(S \odot T) \odot U$ und $S \odot (T \odot U)$ in G liegen. Ist $S \odot T = U$, so folgt, dass $S = T = U$ ist. In diesem Falle gilt also (d). Enthält $S \odot T$ einen Punkt, der von U verschieden ist, so ist $S \neq U$ oder $T \neq U$. Ist $S \neq U$, so folgt

$$G = S \odot U \subseteq (S \odot T) \odot U \subseteq G$$

und

$$G = S \odot U \subseteq S \odot (T \odot U) \subseteq G,$$

so dass (d) auch in diesem Falle gilt. Ist $T \neq U$, so folgt (d) entsprechend.

Es bleibt der Fall zu betrachten, dass S, T und U nicht kollinear sind. Dann sind sie insbesondere auch paarweise verschieden. Wir zeigen zunächst, dass $S \odot (T \odot U) \subseteq (S \odot T) \odot U$ gilt. Dazu sei $A \in S \odot (T \odot U)$. Auf Grund von (a)

dürfen wir annehmen, dass $A \notin S \odot T, U$ gilt. Wegen $A \in S \odot (T \odot U)$ gibt es ein $B \in T \odot U$ mit $A \leq S + B$. Wäre $B = T$, so wäre $A \leq S + T$ im Widerspruch zu $A \notin S \odot T$. Also ist B ein von T verschiedener Punkt in $T \odot U = T + U$, so dass insbesondere $T + U = T + B$ ist. Hieraus folgt weiter, dass B, S und T nicht kollinear sind. Weil $A \neq U$ ist, gibt es nach (P2) daher einen Punkt C auf $S + T$ mit $C \leq A + U$. Nun ist $S + (T \cap T) + U = T$, so dass $C \neq U$ ist. Hiermit folgt zusammen mit $S + T = S \odot T$, dass

$$A \leq A + U = C + U = C \odot U \subseteq (S \odot T) \odot U$$

ist. Damit haben wir gezeigt, dass $S \odot (T \odot U) \subseteq (S \odot T) \odot U$ gilt. Mit (b) folgt nun

$$(S \odot T) \odot U = U \odot (T \odot S) \subseteq (U \odot T) \odot S = S \odot (T \odot U).$$

Also ist in diesem Falle tatsächlich $S \odot (T \odot U) = (S \odot T) \odot U$.

S, T und U seien nun beliebige Punktmengen. Ist eine von ihnen leer, so ist (d) sicherlich erfüllt. Wir dürfen daher annehmen, dass keine von ihnen leer ist. Ist $P \in (S \odot T) \odot U$, so gibt es also Punkte A, B und C mit $A \in S$, $B \in S$, $B \in T$ und $C \in U$ sowie $P \in (A \odot B) \odot C$. Mit dem bereits Bewiesenen und (a) folgt

$$P \in A \odot (B \odot C) \subseteq S \odot (T \odot U),$$

so dass $(S \odot T) \odot U \subseteq S \odot (T \odot U)$ ist. Hieraus folgt unter Benutzung von (b), dass

$$S \odot (T \odot U) = (U \odot T) \odot S \subseteq U \odot (T \odot S) = (S \odot T) \odot U$$

ist. Damit ist (d) bewiesen.

Genau dann ist $S \in L(\Sigma)$, wenn S mit zwei verschiedenen Punkten stets auch ihre Verbindungsgerade enthält. Dies bedeutet, dass S genau dann in $L(\Sigma)$ liegt, wenn $S \odot S \subseteq S$ ist. Aus (a) folgt aber, dass stets $S \subseteq S \odot S$ gilt. Somit ist S genau dann ein Unterraum von Σ, wenn $S \odot S = S$ ist. Dies beweist (e).

Es seien S und T Unterräume von Σ. Nach (c) gilt dann $S \odot T \subseteq S + T$. Mittels (b), (d) und (e) folgt

$$S \odot T \odot S \odot T = S \odot S \odot T \odot T = S \odot T,$$

so dass $S \odot T$ nach (e) ein Unterraum ist. Wegen $S, T \subseteq S \odot T$ gilt nach 1.2 daher $S + T \subseteq S \odot T$, so dass auch (f) richtig ist. Damit ist alles bewiesen.

Es sei Δ eine Menge und $\prec$ sei eine binäre Relation auf Δ, die reflexiv und transitiv sei. Wir nennen Δ bezüglich $\prec$ *gerichtet*, wenn es zu $\alpha, \beta \in \Delta$ stets ein $\gamma \in \Delta$ gibt mit $\alpha \prec \gamma$ und $\beta \prec \gamma$. Prominentestes, nicht triviales Beispiel für diese Situation ist die Menge $\mathrm{Fin}(M)$ der endlichen Teilmengen einer Menge M, die bezüglich der Inklusion gerichtet ist, da die Vereinigung zweier endlicher Mengen wieder endlich ist.

Ist Σ eine projektive Geometrie und ist $M \subseteq L(\Sigma)$ bezüglich der auf $L(\Sigma)$ definierten Relation $\leq$ gerichtet, so nennen wir M *aufsteigendes System* von Unterräumen von Σ. Es gilt nun

1.4. Satz. *Ist Σ eine projektive Geometrie und ist M ein aufsteigendes System von Teilräumen von Σ, so ist*

$$\sum_{X \in M} X = \bigcup_{X \in M} X.$$

Beweis. Es seien P und Q zwei Punkte aus $\bigcup_{X \in M} X$. Es gibt dann Y, $Z \in M$ mit $P \leq Y$ und $Q \leq Z$. Weil M gerichtet ist, gibt es ein $U \in M$ mit Y, $Z \leq U$. Es folgt

$$P + Q \leq U \leq \bigcup_{X \in M} X.$$

Folglich ist $\bigcup_{X \in M} X$ ein Teilraum von Σ. Da dieser Teilraum in $\sum_{X \in M} X$ liegt, folgt mit 1.2 die Gleichheit dieser beiden Räume.

Es sei M eine Teilmenge der Potenzmenge $P(\Pi)$ von Π, wobei Π wieder die Punktmenge einer projektiven Geometrie sei. Ist M endlich, so ist klar, da $\odot$ assoziativ und kommutativ ist, was wir unter

$$\bigodot_{X \in M} X.$$

zu verstehen haben. Wegen 1.3 (a) gilt

$$\bigodot_{X \in M} X = \bigcup_{N \subseteq M} \bigodot_{X \in N} X.$$

Ist M eine nicht notwendig endliche Teilmenge von $P(\Pi)$, so setzen wir den obigen Sachverhalt benutzend

$$\bigodot_{X \in M} X := \bigcup_{N \in \mathrm{Fin}(M)} \bigodot_{X \in N} X.$$

Damit sind wir nun in der Lage, die versprochene interne Beschreibung der Summe von Unterräumen zu geben.

1.5. Satz. *Ist Σ eine projektive Geometrie und ist M eine Teilmenge von $L(\Sigma)$, so ist*

$$\sum_{X \in M} X = \bigodot_{X \in M} X.$$

Beweis. Induktion nach $|M|$ zeigt unter Verwendung von 1.3 (f), dass der Satz richtig ist, falls M endlich ist. Daher ist in jedem Falle

$$\left\{ \bigodot_{X \in N} X \;\middle|\; N \in \mathrm{Fin}(M) \right\}$$

ein aufsteigendes System von Teilräumen von Σ, so dass $\bigodot_{X \in M} M$ nach Satz 1.4 ein Teilraum ist. Mittels Satz 1.2 folgt schließlich die Behauptung.

Als nächstes beweisen wir die Gültigkeit eines eingeschränkten Distributivgesetzes in $L(\Sigma)$. Dieses hat Dedekind als Erster betrachtet, so dass es heute seinen Namen trägt (Dedekind 1897).

1.6. Dedekindsches Modulargesetz. *Es sei Σ eine projektive Geometrie. Sind S, T, $U \in L(\Sigma)$ und ist $T \leq S$, so ist $S \cap (T + U) = T + (S \cap U)$.*

Beweis. Die Gleichung ist richtig, falls T oder U leer ist. Wir dürfen daher annehmen, dass dies nicht der Fall ist.

Es ist ferner trivial, dass $T + (S \cap U) \leq S \cap (T + U)$ ist. Es sei also A ein Punkt von $S \cap (T + U)$. Ist $A \leq T$, so ist nichts zu beweisen. Wir dürfen also $A \not\leq T$ annehmen. Nun ist $A \leq T + U$ und nach 1.3(f) ist $T + U = T \odot U$. Weil T und U nicht leer sind, gibt es dann zwei Punkte B und C mit $B \leq T$, $C \leq U$ und $A \leq B + C$. Wegen $A \not\leq T$ ist $A \neq B$, woraus folgt, dass $B + C = B + A$ ist. Somit ist

$$C \leq A + B \leq S + T = S,$$

da ja $T \leq S$ gilt. Also ist $C \leq S \cap U$. Hieraus folgt schließlich

$$A \leq B + C \leq T + (S \cap U),$$

was zu beweisen war.

Eine weitere wichtige, wenn auch banal zu beweisende Eigenschaft einer projektiven Geometrie wird im nächsten Satz formuliert.

1.7. Satz. *Es sei M ein aufsteigendes System von Teilräumen des projektiven Raumes Σ. Ist dann $Y \in L(\Sigma)$, so ist $Y \cap \sum_{X \in M} X = \sum_{X \in M}(Y \cap X)$.*

Beweis. Mittels Satz 1.4 folgt, da ja auch $\{Y \cap X \mid X \in M\}$ ein aufsteigendes System von Teilräumen ist,

$$Y \cap \sum_{X \in M} X = Y \cap \bigcup_{X \in M} X = \bigcup_{X \in M} (Y \cap X) = \sum_{X \in M} (Y \cap X).$$

1.8. Satz. *Es sei Σ eine projektive Geometrie. Sind X, $Y \in L(\Sigma)$ und gilt $X \cap Y = \emptyset$, so gibt es ein $Z \in L(\Sigma)$ mit $Y \leq Z$, $X \cap Z = \emptyset$ und $X + Z = \Pi$, wobei Π wieder die Menge aller Punkte von Σ bezeichne.*

Beweis. Es sei $N := \{U \mid U \in L(\Sigma), Y \leq U, X \cap U = \emptyset\}$. Dann ist N nicht leer, da Y zu N gehört. Es sei $M \subseteq N$ ein aufsteigendes System von Unterräumen von Σ. Nach 1.4 ist dann $V := \bigcup_{U \in M} U$ ein Teilraum von Σ, der natürlich Y enthält. Weil V die mengentheoretische Vereinigung der U aus M ist, folgt, dass der Schnitt von V mit X leer ist. Somit gilt $V \in N$. Auf Grund des zornschen Lemmas gibt es daher einen maximalen Teilraum Z in N. Es sei $P \in \Pi$. Wir müssen zeigen, dass P in $X + Z$ liegt. Dazu dürfen wir annehmen, dass P weder zu X noch zu Z gehört. Dann ist insbesondere $Y \leq Z < Z + P$, so dass die Maximalität von Z impliziert, dass $X \cap (Z + P) \neq \emptyset$ ist. Es gibt also einen Punkt Q mit $Q \leq X \cap (Z + P)$. Weil P nicht in X liegt, ist Q von P verschieden. Ferner ist $Z + P = Z \odot P$. Es gibt daher einen Punkt R mit $R \leq Z$ und $Q \leq R + P$. Wegen $Q \leq X$ und $X \cap Z = \emptyset$ ist $Q \neq R$. Also ist

$R + P = Q + R$. Daher ist $P \leq Q + R \leq X + Z$. Dies zeigt, dass in der Tat $X + Z = \Pi$ ist.

1.9. Korollar. *Ist $X \in L(\Sigma)$, so gibt es ein $Z \in L(\Sigma)$ mit $X \cap Z = \emptyset$ und $X + Z = \Pi$.*

Beweis. Dies folgt mit $Y := \emptyset$ aus 1.8.

Ist Σ eine projektive Geometrie, sind X, Y, $Z \in L(\Sigma)$ und gilt $X \cap Y = \emptyset$ und $X + Y = Z$, so nennen wir Y *Komplement* von X in Z. Diesen Sachverhalt beschreiben wir, wie in der Algebra üblich, durch $X \oplus Y = Z$.

1.10. Satz. *Es sei Σ eine projektive Geometrie und Π ihre Punktmenge. Ist $\Pi = X \oplus Y$ und ist Y das einzige Komplement von X, so ist $\Pi = X \cup Y$.*

Beweis. Es sei $P \in \Pi$ und $P \notin X$. Nach 1.8 gibt es ein Komplement Z von X mit $P \leq Z$. Weil Y das einzige Komplement von X ist, ist $Z = Y$. Damit ist alles bewiesen.

1.11. Korollar. *Es sei Σ eine projektive Geometrie. Trägt jede Gerade von Σ wenigstens drei Punkte, so sind $\emptyset$ und Π die einzigen Unterräume von Σ, die genau ein Komplement besitzen.*

Beweis. Es sei $\Pi = X \oplus Y$ und X und Y seien beide nicht leer. Ist dann P ein Punkt auf X und Q ein Punkt auf Y, so enthält die Gerade $P + Q$ noch einen dritten Punkt R. Wegen $X \cap Y = \emptyset$ ist $P + Q$ weder in X noch in Y enthalten. Folglich liegt R weder in X noch in Y. Nach 1.10 ist Y daher nicht das einzige Komplement von X.

Es sei $\leq$ eine Teilordnung auf der Menge L und $\leq'$ eine solche auf der Menge L'. Die Bijektion σ von L auf L' heißt *Isomorphismus* von $(L, \leq)$ auf $(L', \leq')$, wenn für alle x, $y \in L$ genau dann $x \leq y$ gilt, wenn $x^\sigma \leq' y^\sigma$ ist.

Ist V ein K-Vektorraum, so bezeichnen wir mit $L(V)$ die Menge seiner Unterräume. Ferner setzen wir

$$\Sigma(V) := \big(UR_1(V), UR_2(V), \subseteq\big).$$

Es gilt dann der folgende Satz, dessen Beweis dem Leser als Übungsaufgabe überlassen bleibe.

1.12. Satz. *Es sei V ein K-Vektorraum. Setze $X^\sigma := \mathrm{UR}_1(X)$ für alle $X \in L(V)$. Dann ist σ ein Isomorphismus von $(L(V), \subseteq)$ auf $(L(\Sigma(V)), \leq)$.*

In Kapitel II werden wir sehen, dass die projektiven Geometrien, deren Rang mindestens 4 ist, alle von dieser Art sind.

2. Projektive Verbände

Als Nächstes geht es darum, die Menge der Unterräume einer projektiven Geometrie verbandstheoretisch zu charakterisieren.

Es sei L eine Menge und $\leq$ sei eine Teilordnung, dh. eine reflexive, antisymmetrische und transitive Relation auf L. Gibt es in L ein Element Π mit

$X \leq \Pi$ für alle $X \in L$, so nennen wir Π das *größte Element* von L. Hat das Element $0 \in L$ die Eigenschaft, dass $0 \leq X$ gilt für alle $X \in L$, so nennen wir 0 das *kleinste Element* von L. Aus der Antisymmetrie der Relation $\leq$ folgt, dass eine teilweise geordnete Menge höchstens ein größtes und höchstens ein kleinstes Element besitzt.

Ist $M \subseteq L$ und ist R eine Element von M, so dass $X \in M$ und $R \leq X$ impliziert, dass $R = X$ ist, so heißt R *maximales Element* von M. Entsprechend werden *minimale Elemente* definiert. Ist $S \in L$ und ist $X \leq S$ für alle $X \in M$, so heißt S *obere Schranke* von M. *Untere Schranken* werden entsprechend definiert. Hat schließlich die Menge der oberen Schranken von M ein kleinstes Element, so heißt dieses Element *obere Grenze* von M. Besitzt M eine obere Grenze, so bezeichnen wir diese mit $\sum_{X \in M} X$. Besitzt die Menge aller unteren Schranken von M ein größtes Element, so heißt dieses Element *untere Grenze* von M. Wir bezeichnen sie mit $\bigcap_{X \in M} X$. Obere und untere Grenzen sind, falls sie existieren, eindeutig bestimmt.

Ist L eine teilweise geordnete Menge und besitzt jede nicht leere endliche Teilmenge von L eine untere und eine obere Grenze, so heißt L *Verband*. Hat jede Teilmenge von L eine obere und eine untere Grenze, so heißt L *vollständiger Verband*. Ein vollständiger Verband besitzt stets ein größtes und ein kleinstes Element, nämlich $\Pi := \sum_{X \in L} X$ und $0 := \bigcap_{X \in L} X$.

Bei der Definition des vollständigen Verbandes haben wir des Guten zuviel getan, wie der folgende Satz zeigt.

2.1. Satz. *Ist L eine teilweise geordnete Menge, so sind die folgenden Aussagen äquivalent:*
(a) *L ist ein vollständiger Verband.*
(b) *Jede Teilmenge von L hat eine untere Grenze.*
(c) *Jede Teilmenge von L hat eine obere Grenze.*

Beweis. (b) und (c) folgen natürlich aus (a).

Es gelte (b) und es sei $M \subseteq L$. Mit M^* bezeichnen wir die Menge der oberen Schranken von M und mit M^{**} bezeichnen wir die Menge der unteren Schranken von M^*. Dann ist natürlich $M \subseteq M^{**}$. Nach Voraussetzung besitzt M^* eine untere Grenze U. *Per definitionem* ist U das größte Element von M^{**}, so dass insbesondere $X \leq U$ gilt für alle $X \in M$. Folglich ist $U \in M^*$. Wegen $U \leq Y$ für alle $Y \in M^*$ ist U das kleinste Element in M^*, so dass U eine obere Grenze von M ist. Damit ist gezeigt, dass L ein vollständiger Verband ist.

Ganz entsprechend zeigt man, dass (a) auch aus (c) folgt.

Es sei L ein Verband mit kleinstem Element 0. Genau die minimalen Elemente von $L - \{0\}$ heißen *Atome* von L. Solche braucht es nicht zu geben. Gibt es jedoch zu jedem $X \in L - \{0\}$ ein Atom A mit $A \leq X$, so heißt der Verband L *atomar*.

Es sei L ein Verband mit kleinstem Element 0 und größtem Element Π. Sind $A, B \in L$ und ist $A + B = \Pi$ sowie $A \cap B = 0$, so heißt B *Komplement* von A. Diesen Sachverhalt bezeichnen wir wie schon zuvor mit $\Pi = A \oplus B$. Hat jedes Element von L ein Komplement, so heißt L *komplementärer* Verband. Der

Verband L heißt *irreduzibel*, falls 0 und Π die einzigen Elemente von L sind, die genau ein Komplement haben.

Der Verband L heißt *modular*, falls aus A, B, $C \in L$ und $B \leq A$ folgt, dass $A \cap (B + C) = B + (A \cap C)$ folgt.

Es sei L ein Verband und M sei eine Teilmenge von L. Ist M bezüglich der auf L gegebenen Teilordnung gerichtet, so nennen wir M ein *aufsteigendes System*. Der Verband L heißt nach *oben stetig*, falls alle aufsteigenden Systeme von L eine obere Grenze haben und falls für alle aufsteigenden Systeme M und alle $Y \in L$ gilt, dass $Y \cap \sum_{X \in M} X = \sum_{X \in M} (Y \cap X)$ ist.

Einen vollständigen, atomaren, modularen, komplementären und nach oben stetigen Verband nennen wir *projektiv*. Die Ergebnisse des ersten Abschnitts lassen sich nun zusammenfassen zu

2.2. Satz. *Ist Σ eine projektive Geometrie, so ist $L(\Sigma)$ bezüglich der Inklusion als Teilordnung ein projektiver Verband.*

Das Hauptziel dieses Abschnittes ist nun zu zeigen, dass jeder projektive Verband zum Unterraumverband einer projektiven Geometrie isomorph ist.

Es sei L ein Verband und C, $D \in L$. Ferner sei $C \leq D$. Wir setzen

$$D/C := \{X \mid X \in L,\ C \leq X \leq D\}$$

und nennen D/C den *Quotienten* von D nach C. Offenbar ist D/C bezüglich der in L definierten Teilordnung ein Verband, m. a. W., D/C ist ein *Teilverband* von L.

2.3. Transformationsregel. *Es sei L ein modularer Verband und A und B seien Elemente von L. Setze*

$$X^\sigma := X \cap B \text{ für } X \in (A + B)/A$$

und

$$Y^\tau := Y + A \text{ für } Y \in B/(A \cap B).$$

Dann ist σ ein Isomorphismus von $(A + B)/A$ auf $B/(A \cap B)$ und τ ist ein Isomorphismus von $B/(A \cap B)$ auf $(A + B)/A$. Überdies sind σ und τ invers zueinander.

Beweis. Aus $A \leq X$ folgt $A \cap B \leq X \cap B \leq B$, so dass σ eine Abbildung von $(A + B)/A$ in $B/(A \cap B)$ ist. Ist $A \cap B \leq Y \leq B$, so folgt $A \leq Y + A \leq A + B$, so dass τ eine Abbildung von $B/(A \cap B)$ in $(A + B)/A$ ist.

Ist $A \leq X \leq A + B$, so folgt auf Grund der Modularität von L, dass

$$X^{\sigma\tau} = (X \cap B) + A = X \cap (A + B) = X$$

ist. Folglich ist $\sigma\tau$ die Identität auf $(A + B)/A$. Ist $A \cap B \leq Y \leq B$, so folgt wiederum wegen der Modularität von L, dass

$$Y^{\tau\sigma} = (Y + A) \cap B = Y + (A \cap B) = Y$$

ist. Also ist $\tau\sigma$ die Identität auf $B/(A \cap B)$. Folglich sind σ und τ zueinander inverse Bijektionen.

Schließlich folgt aus $A \leq X_1 \leq X_2 \leq A + B$, dass $X_1^\sigma = X_1 \cap B \leq X_2 \cap B = X_2^\sigma$ ist, und aus $A \cap B \leq Y_1 \leq Y_2 \leq B$ folgt, dass auch $Y_1^\tau = Y_1 + a \leq Y_2 + A = Y_2^\tau$ gilt. Damit ist alles bewiesen.

2.4. Korollar. *Ist P ein Atom des modularen Verbandes L, dessen kleinstes Element wieder mit 0 bezeichnet sei, und ist $A \in L$, so ist entweder $P \leq A$ oder $(A + P)/A$ und $P/0$ sind isomorph.*

Beweis. Nach 2.3 sind $(A + P)/A$ und $P/(A \cap P)$ isomorph. Nun ist $0 \leq A \cap P \leq P$ und daher, da P ein Atom ist, entweder $A \cap P = 0$ oder $A \cap P = P$, dh., $P \leq A$.

2.5. Korollar. *Es sei L ein modularer Verband mit kleinstem Element 0. Sind P, Q und R Atome von L, ist $R \neq P$ und $R \leq P + Q$, so ist $P + Q = P + R$.*

Beweis. Es ist $P \neq Q$, da sonst $P = Q = R$ wäre. Somit ist $(P + Q)/P$ nach 2.4 zu $Q/0$ isomorph. Da der Quotient $Q/0$ nur aus den Elementen 0 und Q besteht, enthält der Quotient $(P + Q)/P$ nur die beiden Elemente P und $P + Q$. Hieraus folgt, dass $P + R = P + Q$ ist, da ja $P < P + R \leq P + Q$ ist.

2.6. Satz. *Es sei L ein modularer Verband mit kleinstem Element 0. Ferner seien P und Q zwei verschiedene Atome von L. Schließlich sei $A \in L$ und $Q \leq P + A$. Ist $Q \leq A$, so setzen wir $R := Q$. Ist $Q \not\leq A$, so setzen wir $R := A \cap (P + Q)$. Dann ist R ein Atom und es gilt $R \leq A$ und $Q \leq P + R$.*

Beweis. Ist $Q \leq A$, so ist nichts zu beweisen. Es sei also $Q \not\leq A$. Dann ist auch $P \not\leq A$, da andernfalls $Q \leq P + A = A$ wäre. Es folgt $P \cap A = 0$ und weiter

$$P/0 = P/(P \cap A) \cong (A + P)/A = (A + P + Q)/A \cong (P + Q)/R.$$

Somit ist $(P + Q)/R = \{R, P + Q\}$ und $R \neq P + Q$. Andererseits ist

$$(R + P)/R \cong P/(P \cap R) = P/0,$$

da ja $P \cap R \leq P \cap A = 0$ ist. Also ist $(R + P) = \{R, P + R\}$ und $R \neq P + R$. Nun ist aber $R + P \leq P + Q + P = P + Q$ und folglich $(R + P)/R \subseteq (P + Q)/R$. Hieraus folgt zusammen mit dem bereits Bewiesenen, dass $\{R, P + R\} = \{R, P + Q\}$ und damit dass $P + Q = P + R$ ist. Damit ist zunächst gezeigt, dass $Q \leq P + R$ ist.

Es bleibt zu zeigen, dass R ein Atom ist. Dies folgt nun aus

$$R/0 = R/(P \cap R) \cong (R + P)/P = (Q + P)/P \cong Q/(P \cap Q) = Q/0,$$

wobei wir erst hier die Voraussetzung $P \neq Q$ benutzt haben.

Der nächste Satz ist der verbandstheoretische Hintergrund des Veblen-Young Axioms.

2.7. Satz. *Es sei L ein modularer Verband mit 0 und P, Q und R seien drei verschiedene Atome von L mit $R \not\leq P + Q$. Sind dann S und T zwei verschiedene*

Atome mit $S \leq P + Q$ *und* $T \leq Q + R$*, so gibt es ein Atom* U *mit* $U \leq S + T$ *und* $U \leq R + P$.

Beweis. Ist $S = P$, so tut's $U := P$. Es sei also $S \neq P$. Nun ist $S \leq P + Q$. Nach 2.5 ist daher $P + Q = P + S$. Also ist $Q \leq P + S$. Hieraus folgt, dass $T \leq Q + R \leq S + P + R$ ist. Aus 2.6. folgt schließlich, dass es ein Atom U gibt mit $U \leq P + R$ und $T \leq S + U$. Weil $T \neq S$ ist, folgt wiederum aus 2.5, dass $S + U = S + T$ ist. Also ist auch $U \leq S + T$. Damit ist alles bewiesen.

Für spätere Verwendung beweisen wir den nächsten Satz, der auf der Menge der Atome eines modularen Verbandes eine Äquivalenzrelation beschreibt. Bei seinem Beweis wird der gerade bewiesene Satz benutzt.

2.8. Satz. *Es sei* L *ein modularer Verband mit kleinstem Element* 0. *Sind* P *und* Q *Atome von* L*, so setzen wir* $P \sim Q$ *genau dann, wenn entweder* $P = Q$ *ist oder wenn* $P + Q$ *wenigstens drei Atome umfasst. Dann ist* $\sim$ *eine Äquivalenzrelation auf der Menge der Atome von* L.

Beweis. Die Relation $\sim$ ist offenkundig reflexiv und symmetrisch. Um die Transitivität zu beweisen, seien P, Q und R drei Atome von L und es gelte $P \sim Q$ und $Q \sim R$. Sind zwei der drei Atome gleich, so ist nichts zu beweisen. Wir dürfen daher annehmen, dass sie paarweise verschieden sind. Ist $R \leq P+Q$, so folgt $P+R = P+Q$. Hieraus folgt, dass $P+R$ mindestens drei Atome enthält, so dass $P \sim R$ gilt. Es sei schließlich $R \not\leq P + Q$. Wegen $P \sim Q$ und $Q \sim R$ gibt es ein von P und Q verschiedenes Atom A mit $A \leq P + Q$ und ein von Q und R verschiedenes Atom B mit $B \leq Q + R$. Nach 2.7 gibt es ein Atom C mit $C \leq A + B$ und $C \leq R + P$. Es bleibt zu zeigen, dass C von P und R verschieden ist. Wäre $C = P$, so folgte $C + A = P + A \leq P + Q$ und damit $C + A = P + Q$, da ja $P \neq A$ ist. Aus $C \leq A + B$ folgte weiter $C + A = A + B$ und daher

$$B \leq (P + Q) \cap (Q + R) = Q.$$

Dieser Widerspruch zeigt, dass $C \neq P$ ist. Ganz entsprechend zeigt man, dass auch $C \neq R$ gilt. Damit ist alles bewiesen.

Es sei L ein Verband mit kleinstem Element 0. Der Verband L heißt *relativ atomar*, wenn es zu A, $B \in L$ mit $B < A$ stets ein Atom P gibt mit $B < B + P \leq A$.

2.9. Satz. *Es sei* L *ein Verband mit kleinstem Element* 0. *Ist* L *relativ atomar, so ist jedes Element von* L *die obere Grenze der in ihm enthaltenen Atome.*

Beweis. Es sei A ein von 0 verschiedenes Element von L und S sei die Menge der in A enthaltenen Atome. Dann ist A eine obere Schranke von S. Es sei B eine weitere obere Schranke von S. Dann ist auch $B \cap A$ eine obere Schranke von S. Wäre $B \cap A < A$, so gäbe es ein Atom P mit $B \cap A < (B \cap A) + P \leq A$. Es folgte $P \in S$ und damit der Widerspruch $P \leq B \cap A$. Also ist $A = A \cap B \leq B$. Somit ist A die kleinste obere Schranke von S, was zu beweisen war.

Der Verband L heißt *relativ komplementär*, wenn jeder Quotient zweier Elemente von L ein komplementärer Verband ist, dh., wenn es zu U, V, $W \in L$ mit $U \leq V \leq W$ stets ein $X \in L$ gibt mit $V \cap X = U$ und $V + X = W$.

2.10. Satz. *Es sei L ein komplementärer und modularer Verband mit größtem Element Π und kleinstem Element 0. Ferner seien U, V und W drei Elemente von L mit $U \leq V \leq W$ und Y sei ein Komplement von V in Π. Setze $X := U + (Y \cap W)$. Dann ist $X \cap V = U$ und $X + V = W$. Mit anderen Worten, jeder komplementäre, modulare Verband ist relativ komplementär.*

Beweis. Es ist $V + X = V + U + (Y \cap W) = V + (Y \cap W)$. Wegen der Modularität von L ist daher

$$V + X = W \cap (V + Y) = W.$$

Andererseits ist, wiederum auf Grund der Modularität von L,

$$\begin{aligned} V \cap X &= V \cap (U + (Y \cap W)) \\ &= U + \big(V \cap Y \cap W\big) = U + (0 \cap W) = U. \end{aligned}$$

Damit ist alles bewiesen.

2.11. Satz. *In einem atomaren, komplementären und modularen Verband ist jedes Element die obere Grenze der in ihm enthaltenen Atome.*

Beweis. Nach 2.9 genügt es zu zeigen, dass jeder solche Verband relativ atomar ist. Dies folgt aber unmittelbar aus der in Satz 2.10 etablierten relativen Komplementarität eines komplementären modularen Verbandes.

An dieser Stelle ist eine methodische Bemerkung angebracht. Ist Σ eine projektive Geometrie, so ist $L(\Sigma)$ auf Grund seiner Definition natürlich relativ atomar. Man benötigt also nicht die relative Komplementarität dieses Verbandes, um dies festzustellen. Dies wäre mit Kanonen nach Spatzen geschossen, da man die Komplementarität von $L(\Sigma)$ nur über das zornsche Lemma erhält.

2.12. Satz von der endlichen Abhängigkeit. *Es sei L ein relativ atomarer, vollständiger Verband. Genau dann ist L nach oben stetig, wenn gilt: Ist P ein Atom und S eine Menge von Atomen von L, ist ferner $P \leq \sum_{Q \in S} Q$, so gibt es endliche viele Punkte $Q_1, \ldots, Q_t$ in S mit $P \leq \sum_{i:=1}^{t} Q_i$.*

Beweis. Es sei L nach oben stetig. Ferner sei P ein Atom und S eine Menge von Atomen von L und es gelte $P \leq \sum_{Q \in S} Q$. Das System $M := \{\sum_{Q \in \Phi} Q \mid \Phi \in \mathrm{Fin}(S)\}$ ist aufsteigend. Ferner ist $\sum_{X \in M} X = \sum_{Q \in S} Q$. Folglich ist

$$P = P \cap \sum_{Q \in S} Q = P \cap \sum_{X \in M} X = \sum_{X \in M} (P \cap X).$$

Hieraus folgt die Existenz eines $X \in M$ mit $P \cap X \neq 0$. Weil P ein Atom ist, folgt weiter $P \leq X$. Weil X von einer endlichen Teilmenge von S erzeugt wird, gibt es also endlich viele $Q_1, \ldots, Q_t \in S$ mit $P \leq \sum_{i:=1}^{t} Q_i$.

Umgekehrt gelte: Wann immer P ein Atom und S eine Menge von Atomen von L ist, so dass $P \leq \sum_{Q \in S} Q$ ist, so gibt es endlich viele $Q_1, \ldots, Q_t \in S$ mit $P \leq \sum_{i:=1}^{t} Q_i$. Unter dieser Annahme müssen wir nun zeigen, dass L nach oben stetig ist.

Ist $X \in L$, so bezeichnen wir mit $S(X)$ die Menge der in X enthaltenen Atome. Nach 2.9 ist dann $X = \sum_{Q \in S(X)} Q$. Ferner gilt $S(X) \cap S(Y) = S(X \cap Y)$.

Es sei nun M ein aufsteigendes System von L. Ferner sei $B \in L$. Dann ist

$$\sum_{X \in M} (B \cap X) \leq B \cap \sum_{X \in M} X.$$

Es sei P ein Atom von $B \cap \sum_{X \in M} X$. Dann ist insbesondere

$$P \leq \sum_{X \in M} \sum_{Q \in S(X)} Q.$$

Es gibt also $Q_1, \ldots, Q_t \in \bigcup_{X \in M} S(X)$ mit $P \leq \sum_{i:=1}^{t} Q_i$. Weil M gerichtet ist, gibt es ein $Y \in M$ mit $Q_1, \ldots, Q_t \in Y$. Es folgt

$$P \leq B \cap Y \leq B \cap \sum_{X \in M} X.$$

Weil in einem relativ atomaren Verband jedes Element die obere Grenze seiner Atome ist, folgt schließlich

$$B \cap \sum_{X \in M} X \leq \sum_{X \in M} (B \cap X).$$

Damit ist Satz 2.12 bewiesen. Er wird uns im nächsten Abschnitt gute Dienste leisten.

Nun zeigen wir, dass jeder projektive Verband zum Unterraumverband einer projektiven Geometrie isomorph ist.

2.13. Satz. *Es sei L ein projektiver Verband. Wir definieren eine Inzidenzstruktur Σ wie folgt. Punkte von Σ sind die Atome von L. Geraden von Σ sind die Elemente der Form $P + Q$ von L, wobei P und Q zwei verschiedene Atome von L sind. Dann ist Σ eine projektive Geometrie und die Verbände L und $L(\Sigma)$ sind isomorph.*

Beweis. Durch zwei verschiedene Punkte von Σ geht stets eine Gerade, und aus 2.5 folgt, dass es auch nur eine Gerade durch zwei verschiedene Punkte gibt. Also gilt (P1). Nach 2.7 gilt auch (P2). Schließlich gilt (P3) auf Grund der Definition einer Geraden.

Um die Isomorphie von L und $L(\Sigma)$ zu beweisen, probiere man das Nächstliegende. Funktionierte dies nicht, wäre man in Schwierigkeiten. Für $X \in L$ setzen wir also X^σ gleich der Menge der in X liegenden Atome und für $Y \in L(\Sigma)$ setzen wir $Y^\tau := \sum_{Q \in Y} Q$, wobei $\sum$ die obere Grenze in L bezeichne. Dann ist σ eine Abbildung von L in $L(\Sigma)$ und τ eine Abbildung von $L(\Sigma)$ in L. Ist nun $X \in L$, so ist X die obere Grenze der in X enthaltenen Atome. Daher ist $X^{\sigma\tau} = X$, so dass $\sigma\tau = id_L$ ist.

Es sei $Y \in L(\Sigma)$ und P ein Atom von L mit $P \leq Y^\tau$. Wir zeigen, dass P in Y liegt. Nach dem Satz von der endlichen Abhängigkeit gibt es $Q_1, \ldots,$

$Q_t \in Y$ mit $P \leq \sum_{i:=1}^{t} Q_i$, wobei $\sum$ sich wieder auf L bezieht. Ist $t = 1$, so ist $P = Q_1 \in Y$. Es sei also $t > 1$. Dann ist $P \leq Q_1 + \sum_{i:=2}^{t} Q_i$. Nach Satz 2.6 gibt es einen Punkt R mit $P \leq Q_1 + R$ und $R \leq \sum_{i:=2}^{t} Q_i$. Nach Induktionsannahme ist $R \in Y$. Dann ist aber $Q_1 + R$ eine Gerade von Y, so dass auch $P \in Y$ gilt. Somit ist $Y^{\tau\sigma} = Y$, so dass $\tau\sigma = id_{L(\Sigma)}$ ist. Folglich sind σ und τ zueinander inverse Bijektionen. Dass beide inklusionstreu sind, ist banal.

Die Frage, wann ein projektiver Verband irreduzibel ist, ist nun leicht zu beantworten.

2.14. Satz. *Es sei L ein projektiver Verband. Genau dann ist L irreduzibel, wenn auf jeder Geraden von L wenigstens drei Punkte liegen. Ist L irreduzibel, sind X, $Y \in L$ und gilt $Y \leq X$, so ist auch X/Y irreduzibel.*

Beweis. Nach 2.13 dürfen wir annehmen, dass $L = L(\Sigma)$ ist, wobei Σ wie in 2.13 definiert sei. Liegen nun auf jeder Geraden von Σ drei Punkte, so ist L nach 1.11 irreduzibel.

Es sei L irreduzibel. Ferner sei U eine Äquivalenzklasse der in 2.8 erklärten Äquivalenzrelation $\sim$. Dann ist $U \in L$. Es sei V die Menge der nicht in U liegenden Punkte von σ. Dann ist auch $V \in L$, da V Vereinigung von Äquivalenzklassen von $\sim$ ist. Dann ist $U \cup V = \Pi = U \oplus V$. Hieraus folgt aber, dass V das einzige Komplement von U ist. Da U als Äquivalenzklasse nicht leer ist, ist $U = \Pi$, da L als irreduzibel vorausgesetzt war. Somit ist $V = 0$ und alle Geraden von Σ sind in U enthalten und tragen daher alle mindestens drei Punkte.

Es sei L irreduzibel, es seien $X, Y \in L$ und es gelte $Y \leq X$. Es sei $G \in X/Y$ eine Gerade von X/Y. Weil L relativ komplementär ist, gibt es ein H mit $G = Y \oplus H$. Mittels der Transformationsregel folgt, dass $H/0$ zu G/Y isomorph ist. Also ist H eine Gerade, trägt daher drei verschiedene Punkte P_1, P_2 und P_3. Setze $Q_i := P_i + Y$. Dann sind Q_1, Q_2, Q_3 drei verschieden Punkte von X/Y, die alle auf G liegen. Folglich ist X/Y irreduzibel.

Es sei $(L_i \mid i \in I)$ eine Familie von Verbänden. Wir versehen das cartesische Produkt $C := \mathrm{cart}_{i \in I} L_i$ der L_i mit einer binären Relation $\leq$, indem wir für alle F, $G \in C$ genau dann $F \leq G$ setzen, wenn $F_i \leq G_i$ für alle $i \in I$ gilt. Es ist schnell verifiziert, dass $(C, \leq)$ ebenfalls ein Verband ist. Sind alle L_i projektiv, so ist auch C projektiv.

2.15. Satz. *Es sei L ein projektiver Verband. Auf Grund von 2.13 dürfen wir jedes Element von L mit der Menge der auf ihm liegenden Punkte identifizieren. Es sei Π die Menge aller Punkte von L und 0 bezeichne die leere Menge. Es sei weiter $\Pi/\sim$ die Menge der Äquivalenzklassen der in 2.8 definierten Äquivalenzrelation $\sim$. Ist dann $U \in \Pi/\sim$, so ist $U \in L$ und der Quotient $U/0$ ist mit der von L ererbten Teilordnung ein irreduzibler projektiver Verband. Ist nun $X \in L$, so definieren wir*

$$\sigma(X) \in \mathrm{cart}_{U \in \Pi/\sim} U/0$$

durch $\sigma(X)_U := X \cap U$. Dann ist σ ein Isomorphismus von L auf $\mathrm{cart}_{U \in \Pi/\sim} U/0$.

Beweis. Natürlich ist σ eine Abbildung von L in das fragliche cartesische Produkt, welches wir abkürzend mit C bezeichnen. Es sei $\sigma(X) = \sigma(Y)$. Dann ist

$$\begin{aligned} X = X \cap \bigcup_{U \in \Pi/\sim} U &= \bigcup_{U \in \Pi/\sim} X \cap U \\ = \bigcup_{U \in \Pi/\sim} Y \cap U &= Y \cap \bigcup_{U \in \Pi/\sim} U = Y. \end{aligned}$$

Dies zeigt, dass σ injektiv ist. Um zu zeigen, dass σ auch surjektiv ist, sei $F \in C$. Wir setzen $X := \cup_{U \in \Pi/\sim} F_U$. Sind P und Q zwei verschiedene Punkte von X, so liegt auch $P + Q$ ganz in X: Dies ist sicherlich richtig, wenn P und Q in ein und demselben F_U liegen. Liegen sie aber in verschiedenen Äquivalenzklassen, so liegen auf $P + Q$ nur die beiden Punkte P und Q. Somit gilt $X \in L$. Da nun $\sigma(X) = F_U$ ist, ist σ auch surjektiv.

Die Inklusionstreue von σ ist banal.

Dieser Satz zeigt, dass man alle projektiven Verbände kennt, wenn man nur die irreduziblen unter ihnen kennt.

3. Der Basissatz

Die Vorgehensweise in diesem Abschnitt mag dem ein oder anderen Leser umständlich erscheinen. Sie erklärt sich daraus, dass ich immer versuche, ohne das Auswahlaxiom auszukommen.

Es sei L ein projektiver Verband, dessen Punktmenge wir wieder mit Π bezeichnen. Wir nennen $X \in L$ *endlich erzeugt*, wenn es ein $\Phi \in \mathrm{Fin}(\Pi)$ gibt mit $X = \sum_{P \in \Phi} P$. Ist X endlich erzeugt, so setzen wir

$$\mathrm{Rg}_L(X) := \min\bigl\{|\Phi| \bigm| \Phi \in \mathrm{Fin}(\Pi), X = \textstyle\sum_{P \in \Phi} P\bigr\}$$

und lesen $\mathrm{Rg}_L(X)$ als *Rang* von X. Ist Π endlich erzeugt, so nennen wir $\mathrm{Rg}_L(\Pi)$ auch Rang von L. Der Vollständigkeit halber sei erwähnt, dass im Falle der Endlichkeit von $\mathrm{Rg}_L(X)$ die Zahl $\mathrm{Rg}_L(X) - 1$ die *Dimension* von X ist.

3.1. Satz. *Es sei L ein projektiver Verband. Ferner seien X, $Y \in L$ und es gelte $Y \leq X$. Ist X endlich erzeugt, so ist auch Y endlich erzeugt und es gilt* $\mathrm{Rg}_L(Y) \leq \mathrm{Rg}_L(X)$. *Überdies gilt in diesem Falle genau dann* $\mathrm{Rg}_L(Y) = \mathrm{Rg}_L(X)$*, wenn $Y = X$ ist.*

Beweis. Es sei $n := \mathrm{Rg}_L(X)$ und Φ sei eine Menge von n Punkten, die X erzeugt. Ist $n = 0$, so ist $X = 0$ und dann auch $Y = 0$, so dass der Satz in diesem Falle gilt. Es sei also $n > 0$. Ist $Y = X$, so ist nichts zu beweisen. Es sei also $Y < X$. Es gibt dann ein $P \in \Phi$ mit $P \not\leq Y$. Nach der Transformationsregel gilt daher $Y/0 \cong (Y + P)/P$. Ist $Q \in \Phi - \{P\}$, so ist $Q + P$ ein Atom des Quotienten X/P und X ist als Element von X/P das Erzeugnis dieser Atome. Daher ist $\mathrm{Rg}_{X/P}(X) \leq n - 1$. Nach Induktionsannahme ist folglich $Y + P$ als Element von X/P endlich erzeugt und es gilt $\mathrm{Rg}_{X/P}(Y + P) \leq n - 1$. Wegen der Isomorphie von $Y/0$ und $(Y + P)/P$ ist also auch Y endlich erzeugt und die Ungleichung $\mathrm{Rg}_L(Y) \leq n - 1$ erfüllt.

Statt zu sagen, dass X endlich erzeugt sei, werden wir in Zukunft auch sagen, dass X *endlichen Ranges* sei.

Ist Φ eine Menge von Punkten eines projektiven Verbandes L und ist P ein Punkt von L, so heißt P *abhängig* von Φ, falls $P \leq \sum_{Q \in \Phi} Q$ gilt. Hat die Menge Φ von Punkten von L die Eigenschaft, dass keiner ihrer Punkte P von $\Phi - \{P\}$ abhängt, so nennen wir Φ *unabhängig*.

Ist X ein Teilraum endlichen Ranges eines projektiven Verbandes und sind $P_1, \ldots, P_{\mathrm{Rg}_L(X)}$ Punkte, die X erzeugen, so ist die aus diesen Punkten gebildete Menge unabhängig.

3.2. Satz. *Es sei L ein projektiver Verband und X sei ein Teilraum endlichen Ranges von L. Ist Φ eine unabhängige Teilmenge von Punkten von X, so ist Φ endlich und es gilt $|\Phi| \leq \mathrm{Rg}_L(X)$.*

Beweis. Der von Φ erzeugte Unterraum von L ist nach 3.1 endlich erzeugt und sein Rang ist höchstens gleich dem Rang von X. Wir dürfen daher annehmen, dass $X = \sum_{Q \in \Phi} Q$ ist. Setze $n := \mathrm{Rg}_L(X)$. Ist $n = 1$, so ist die Aussage des Satzes offenkundig. Es sei also $n > 1$ und $\{P_1, \ldots, P_n\}$ sei eine Menge von Punkten, die X erzeugt. Setze $Y := \sum_{i:=1}^{n-1} P_i$. Dann ist

$$Y < X = \sum_{Q \in \Phi} Q.$$

Es gibt also ein $Q \in \Phi$ mit $Q \not\leq Y$. Nach der Transformationsregel gilt

$$X/Y = (Y + P_n)/Y \cong P_n/(Y \cap P_n) = P_n/0.$$

Andererseits sind auch $(Y + Q)/Y$ und $Q/0$ isomorph. Weil P_n und Q Punkte sind, sind aber auch $P_n/0$ und $Q/0$ isomorph. Somit sind X/Y und $(Y + Q)/Y$ isomorph. Weil der zweite Quotient im ersten enthalten ist und beide Quotienten nur je zwei Elemente enthalten, gilt schließlich $X = Y + Q$.

Setze $Z := \sum_{R \in \Phi - \{Q\}} R$. Dann ist $Z + Q = X$ und $Z \cap Q = 0$. Also ist

$$Y/0 \cong (Y + Q)/Q = (Z + Q)/Q \cong Z/0.$$

Hieraus folgt $\mathrm{Rg}_L(Z) = \mathrm{Rg}_L(Y) \leq n - 1$. Nach Induktionsannahme ist daher $|\Phi - \{Q\}| \leq n - 1$ und folglich $|\Phi| \leq n$.

3.3. Korollar. *Es sei L ein projektiver Verband und Φ sei eine endliche unabhängige Menge von Punkten. Dann ist*

$$|\Phi| = \mathrm{Rg}_L\bigl(\textstyle\sum_{P \in \Phi} P\bigr).$$

Beweis. Es sei $X := \sum_{P \in \Phi} P$. Dann gilt *per definitionem* die Ungleichung $\mathrm{Rg}_L(X) \leq |\Phi|$. Andererseits gilt nach 3.2 auch $|\Phi| \leq \mathrm{Rg}_L(X)$. Damit ist das Korollar bewiesen.

Die Punkte eines projektiven Verbandes sind genau die Unterräume des Ranges 1 und die Geraden sind die Unterräume des Ranges 2. Die Unterräume

des Ranges 3 nennen wir *Ebenen*. Ferner nennen wir die Komplemente von Punkten *Hyperebenen* und gelegentlich auch *Ko-Atome*.

3.4. Satz. *Es sei L ein projektiver Verband und $U(L)$ sei die Menge der unabhängigen Mengen von Punkten von L. Dann gilt:*

a) *Ist Φ eine Menge von Punkten von L, so gilt genau dann $\Phi \in U(L)$, wenn $\mathrm{Fin}(\Phi) \subseteq U(L)$ gilt.*

b) *Sind $\Phi, \Psi \in U(L)$, sind Φ und Ψ beide endlich und gilt $|\Psi| = |\Phi| + 1$, so gibt es ein $P \in \Psi - \Phi$ mit $\Phi \cup \{P\} \in U(L)$.*

Beweis. a) Ist $\Phi \in U(L)$, so ist natürlich $\mathrm{Fin}(\Psi) \subseteq U(L)$. Es sei Φ abhängig. Es gibt dann ein $P \in \Psi$, so dass P von $\Phi - \{P\}$ abhängt. Nach dem Satz von der endlichen Abhängigkeit gibt es eine endliche Teilmenge Ψ von $\Phi - \{P\}$, so dass P von Ψ abhängt. Es folgt, dass $\Psi \cup \{P\}$ eine endliche abhängige Teilmenge von Φ ist, so dass $\mathrm{Fin}(\Phi) \not\subseteq U(L)$ gilt.

b) Setze $X := \sum_{Q \in \Phi} Q$. Nach 3.2 gibt es dann wegen $|\Psi| > |\Phi|$ ein $P \in \Psi$ mit $P \not\leq X$. Setze $Y := X + P$. Dann ist Y endlich erzeugt und überdies $X < Y$. Nach 3.3 und 3.1 ist daher

$$|\Phi| = \mathrm{Rg}_L(X) < \mathrm{Rg}_L(Y) \leq \left|\Phi \cup \{P\}\right| = |\Phi| + 1.$$

Es folgt $\mathrm{Rg}_L(Y) =| \Phi \cup \{P\} |$, so dass $\Phi \cup \{P\}$ in der Tat unabhängig ist.

Satz 3.4 besagt, dass $U(L)$ ein Beispiel für das ist, was man *Unabhängigkeitsstruktur* nennt. Die Eigenschaft b) wird gewöhnlich *steinitzscher Austauschsatz* genannt.

Es sei X ein Teilraum des projektiven Verbandes L. Ist Φ eine Menge von Punkten von X, so heißt Φ eine *Basis* von X, wenn Φ unabhängig ist und X erzeugt. Ist X endlichen Ranges und ist Φ eine Basis von X, so ist, wie wir oben gesehen haben, $|\Phi| = \mathrm{Rg}_L(X)$. Ferner gilt:

3.5. Basissatz. *Es sei L ein projektiver Verband. Ist $X \in L$ und ist Ψ eine unabhängige Menge von Punkten von X, so gibt es eine Basis Φ von X mit $\Psi \subseteq \Phi$. Insbesondere hat jedes $X \in L$ eine Basis.*

Beweis. Ist X endlichen Ranges, so gibt es *per definitionem* eine Basis Ω von X. Weil $|\Psi| \leq |\Omega|$ gilt, folgt die Existenz von Ψ mittels Induktion aus dem Steinitzschen Austauschsatz.

Ist X nicht endlichen Ranges, so erschließe man die Existenz von Φ mittels des zornschen Lemmas.

Die letzte Aussage dieses Satzes folgt mit $\Psi := \emptyset$ aus dem bereits Bewiesenen.

Weil $U(L)$ eine Unabhängigkeitsstruktur ist, folgt, dass sich zwei Basen eines Elements $X \in L$ stets bijektiv aufeinander abbilden lassen. Wir werden diesen Beweis hier nicht durchführen. Für einen solchen sei der interessierte Leser auf Lüneburg 1989 verwiesen. Die allen Basen von X gemeinsame Kardinalzahl heißt *Rang* von X. Sie werde ebenfalls mit $\mathrm{Rg}_L(X)$ bezeichnet.

3.6. Satz. *Es sei L ein projektiver Verband und X und Y seien Elemente von L. Ferner sei Φ eine Basis von X und Ψ eine Basis von Y. Ist $X \cap Y = 0$, so ist $\Phi \cap \Psi = \emptyset$ und $\Phi \cup \Psi$ ist eine Basis von $X + Y$.*

Beweis. Die Aussage über den Schnitt von Φ mit Ψ ist trivial. Ferner ist klar, dass $X+Y$ von $\Phi \cup \Psi$ erzeugt wird. Es ist zu zeigen, dass $\Phi \cup \Psi$ unabhängig ist. Um dies zu zeigen, setzen wir zunächst $\Omega := \Phi \cup \Psi$. Wäre Ω abhängig, so gäbe es ein $P \in \Omega$, so dass P von $\Omega - \{P\}$ abhinge. Wir könnten oBdA annehmen, dass $P \in \Phi$ gälte. Setzte man dann $Z := \sum_{Q \in \Phi - \{P\}} Q$, so folgte $X + Y = Z + Y$ und weiter, weil L ja modular ist,

$$X = X \cup (Z + Y) = Z + (X \cap Y) = Z$$

im Widerspruch zur Unabhängigkeit von Φ. Damit ist alles gezeigt.

3.7. Rangformel. *Es sei L eine projektiver Verband. Sind X und Y Elemente endlichen Ranges von L, so ist auch $X+Y$ endlichen Ranges und es gilt*

$$\mathrm{Rg}_L(X) + \mathrm{Rg}_L(Y) = \mathrm{Rg}_L(X+Y) + \mathrm{Rg}_L(X \cap Y).$$

Beweis. Weil X und Y endlich erzeugt sind, ist es auch $X+Y$. Es sei W ein Komplement von $X \cap Y$ in Y. Nach 3.6 ist dann

$$\mathrm{Rg}_L(Y) = \mathrm{Rg}_L(X+Y) + \mathrm{Rg}_L(W).$$

Nun ist

$$X + Y = X + (X \cap Y) + W = X + W$$

und

$$X \cap W = X \cap Y \cap W = 0.$$

Also ist $\mathrm{Rg}_L(X+W) = \mathrm{Rg}_L(X) + \mathrm{Rg}_L(W)$. Somit ist

$$\begin{aligned}\mathrm{Rg}_L(X) + \mathrm{Rg}_L(Y) &= \mathrm{Rg}_L(X) + \mathrm{Rg}_L(X \cap Y) + \mathrm{Rg}_L(W)\\ &= \mathrm{Rg}_L(X+Y) + \mathrm{Rg}_L(X \cap Y).\end{aligned}$$

Dieser Beweis funktioniert natürlich auch für unendliche Kardinalzahlen, doch in diesem Falle taugt die Rangformel nicht viel.

4. Vollständig reduzible Moduln

Der Geometrie wird nachgesagt, dass sie von jedem Fortschritt in der Mathematik profitiere, dass sie aber selbst nur wenig bis gar nichts zum Fortschritt der Mathematik beitrage. Dass man die Geometrie jedoch manchmal dazu heranziehen kann, Dinge in anderen Teilen der Mathematik besser zu verstehen, möchte ich hier am Beispiel der vollständig reduziblen Moduln demonstrieren.

Es sei zunächst R ein Ring, wobei wir nicht voraussetzen, dass R eine 1 habe. Es sei ferner M ein R-Rechtsmodul. Mit $L_R(M)$ bezeichnen wir die Menge aller Teilmoduln von M und für die Einschränkung der Inklusionsrelation auf $L_R(M)$ benutzen wir das Symbol $\leq$. Mit diesen Verabredungen gilt nun der folgende Satz.

4.1. Satz. *Ist M ein R-Rechtsmodul, so ist $(L_R(M), \leq)$ ein modularer, vollständiger und nach oben stetiger Verband. Der Schnitt von Teilmoduln im mengentheoretischen Sinne ist gleich ihrem Schnitt im verbandstheoretischen Sinne,*

und ihre Summe im modultheoretischen Sinne stimmt überein mit ihrer Summe im verbandstheoretischen Sinne.

Der simple Beweis dieses Satzes sei dem Leser als Übungsaufgabe überlassen.

Das Rechtsideal I des Ringes R heißt *maximal*, wenn

$$\big|L_R(R/I)\big| = 2$$

ist. Das Rechtsideal I heißt *regulär*, wenn es ein $a \in R$ gibt mit $x - ax \in I$ für alle $x \in R$. Hat R eine Eins, so ist jedes Rechtsideal regulär. Ist I ein reguläres Rechtsideal, und ist J ein Rechtsideal mit $I \subseteq J$, so ist auch J regulär.

Der R-Modul M heißt *irreduzibel*, falls $MR \neq \{0\}$ ist und $L_R(M)$ genau zwei Elemente enthält. Ist M irreduzibel und ist $0 \neq u \in M$, so ist $M = uR$. Ist nämlich $J := \{v \mid v \in M, vR = \{0\}\}$, so ist J ein Teilmodul von M, der wegen $MR \neq \{0\}$ und der Irreduzibilität von M gleich $\{0\}$ ist. Wegen $u \notin J$ ist also $uR = M$.

4.2. Satz. *Es sei R ein Ring und M sei ein irreduzibler R-Modul. Ist $0 \neq u \in M$, so definieren wir den Epimorphismus σ des R-Rechtsmoduls R auf $uR = M$ durch $\sigma(r) := ur$. Dann ist* $\mathrm{Kern}(\sigma)$ *ein maximales, reguläres Rechtsideal von R. Ist umgekehrt I ein maximales, reguläres Rechtsideal von R, so ist R/I ein irreduzibler R-Modul.*

Beweis. Weil M irreduzibel ist, ist $\mathrm{Kern}(\sigma)$ ein maximales Rechtsideal von R. Nun ist $u \in M = uR$. Es gibt also ein $a \in R$ mit $u = ua$. Es folgt $u(r - ar) = 0$ für alle $r \in R$. Somit ist $r - ar \in \mathrm{Kern}(\sigma)$ für alle $r \in R$, so dass $\mathrm{Kern}(\sigma)$ regulär ist.

Es sei jetzt umgekehrt I ein maximales, reguläres Ideal von R. Dann ist $|L_R(R/I)| = 2$. Es sei nun $a \in R$ mit $r - ar \in I$ für alle $r \in R$. Dann ist $A \notin I$, da andernfalls $r \in I$ wäre für alle $r \in R$. Wegen $r + I = ar + I = (a + I)r$ ist daher $(R/I)R = R/I$, so dass R/I irreduzibel ist.

Zwei Eigenschaften fehlen dem Verband $L_R(M)$, um projektiv zu sein, die Komplementarität und die Atomarität, wobei Atome in diesem Zusammenhang die irreduziblen Teilmoduln des R-Moduls M sind. Eine sehr nützliche Charakterisierung dieser Moduln liefert der nächste Satz.

4.3. Satz. *Es sei R ein Ring und M sei ein R-Rechtsmodul. Genau dann ist $L_R(M)$ projektiv, wenn M Summe von irreduziblen Teilmoduln ist.*

Beweis. Es sei M Summe von irreduziblen Teilmoduln. Ferner sei $X \in L_R(M)$. Mittels des zornschen Lemmas erhalten wir ein $Y \in L_R(M)$ maximal bezüglich der Eigenschaft $X \cap Y = \{0\}$. Wir wollen zeigen, dass $X + Y = M$ ist. Dazu nehmen wir an, dies sei nicht der Fall. Weil M Summe von irreduziblen Teilmoduln ist, gibt es einen irreduziblen Teilmodul P von M mit $P \not\leq X + Y$. Es folgt $(X + Y) \cap P = \{0\}$ und dann auch $Y \cap P = \{0\}$. Nun ist $Y \subseteq Y + P$. Mittels der Modularität von $L_R(M)$ folgt daraus

$$(Y + P) \cap (Y + X) = Y + \big(X \cap (Y + P)\big).$$

Andererseits ist $Y \subseteq Y + X$ und daher

$$(Y + X) \cap (Y + P) = Y + \big(P \cap (Y + X)\big) = Y.$$

Aus diesen beiden Gleichungen folgt $Y = Y + (X \cap (Y + P))$, was wiederum $X \cap (Y + P) \subseteq Y$ zur Folge hat. Also gilt

$$X \cap (Y + P) \subseteq X \cap Y = \{0\}.$$

Nun ist $Y \subseteq Y + P$, so dass die Maximalität von Y erzwingt, dass $Y = Y + P$ ist. Dies ergibt aber den Widerspruch $P \leq Y \cap P = \{0\}$. Also ist doch $M = X \oplus Y$, so dass $L_R(M)$ komplementär ist.

Um zu zeigen, dass $L_R(M)$ atomar ist, sei X ein von $\{0\}$ verschiedener Teilmodul von M. Es sei $0 \neq x \in X$. Weil M Summe von irreduziblen Teilmoduln ist, gibt es dann irreduzible Teilmoduln $I_1, \ldots, I_n$ von M mit $x \in \Sigma_{k:=1}^{n} I_k$. Es sei n minimal mit dieser Eigenschaft. Dann ist

$$\sum_{k:=1}^{n} I_k = \bigoplus_{k:=1}^{n} I_k.$$

Zu jedem k gibt es nun ein $i_k \subseteq I_k$ mit $x = \Sigma_{k:=1}^{n} i_k$. Ist nun $r \in R$ und $xr = 0$, so folgt aus der Unabhängigkeit der I_k, dass $i_k r = 0$ ist für alle k. Für $m \in M$ setze man $O(m) := \{r \mid r \in R, mr = 0\}$. Dann folgt aus dem gerade Bewiesenen

$$O(x) \subseteq \bigcap_{k:=1}^{n} O(i_k).$$

Es gilt sogar die Gleichheit, wie man unmittelbar sieht, uns genügt es aber zu wissen, dass $O(x) \subseteq O(i_1)$ gilt. Wegen der Minimalität von n ist $i_1 \neq 0$ und daher $I_1 = i_1 R$. Definiere den Modulhomomorphismus σ von R auf xR durch $\sigma(r) := xr$. Weil $L_r(M)$ als modularer und komplementärer Verband auch relativ komplementär ist, gibt es einen Teilmodul P von xR mit $xR = \sigma(O(i_1)) \oplus P$. Es folgt, dass

$$P \cong xR/\sigma\big(O(i_1)\big) \cong R/O(i_1) \cong I_1$$

ist. Also ist P ein Punkt mit $P \leq xR \leq X$, so dass $L_R(M)$ auch atomar ist.

Ist $L_R(M)$ ein projektiver Verband, so ist jedes Element dieses Verbandes obere Grenze der in ihm enthaltenen Punkte. Insbesondere gilt das für M, so dass M nach 4.1 die Summe irreduzibler Teilmoduln ist. Damit ist der Satz bewiesen.

Hat R eine Eins, so kann man mehr beweisen, da in diesem Falle alle Rechtsideale regulär sind.

4.4. Satz. *Es sei R ein Ring mit Eins und M sei ein unitärer R-Modul. Genau dann ist $L_R(M)$ projektiv, wenn $L_R(M)$ komplementär ist.*

Beweis. Es ist natürlich nur zu zeigen, dass die Komplementarität die Projektivität nach sich zieht.

Es sei also $L_R(M)$ komplementär und X sei ein von $\{0\}$ verschiedener Teilmodul von M. Ferner sei $0 \neq x \in X$. Weil M unitär ist, ist $1 \notin O(x)$. Mit Hilfe des zornschen Lemmas erschließt man die Existenz eines maximalen Rechtsideals I mit $O(x) \subseteq I$. Weil I regulär ist, ist R/I nach 4.2 ein irreduzibler R-Rechtsmodul. Lässt man dieses I die Rolle von $O(i_1)$ im Beweise von 4.3 spielen, so sieht man, dass es einen Punkt P gibt mit $P \leq xR \leq X$. Also ist $L_R(M)$ atomar und damit projektiv.

Ist M ein R-Rechtsmodul, dessen Teilmodulverband projektiv ist, so heißt M *vollständig reduzibel*. Dieser Name ist nicht sehr glücklich gewählt, da er üblicherweise nur beinhaltet, dass jeder Teilmodul von M ein direkter Summand ist. Da wir auch an Ringen ohne Eins interessiert sind, müssen wir unter diesen Begriff auch die Atomarität von $L_R(M)$ subsumieren.

Ist nun M ein vollständig reduzibler R-Modul, so ist Satz 2.15 auf $L_R(M)$ anwendbar. Die interessante algebraische Interpretation dieses Satzes ist Inhalt des nächsten Satzes.

4.5. Satz. *Es sei M ein vollständig reduzibler R-Modul und $I_R(M)$ bezeichne die Menge seiner irreduziblen Teilmoduln. Sind P, $Q \in I_R(M)$, so setzen wir $P \equiv Q$ genau dann, wenn P und Q isomorphe R-Moduln sind. Dann ist $\equiv\, = \,\sim$, wobei $\sim$ wie in 2.8 definiert sei. Für alle $\Phi \in I_R(M)/\!\equiv$ setzen wir*

$$H_\Phi := \sum_{P \in \Phi} P.$$

Dann ist

$$M = \bigoplus_{\Phi \in I_R(M)/\equiv} H_\Phi.$$

Beweis. Wir zeigen, dass $\equiv\, = \,\cong$ ist. Dazu seien A und B zwei verschiedene Elemente aus $I_R(M)$. Dann ist $A \cap B = \{0\}$.

Es gelte $A \equiv B$. Es gibt dann einen Isomorphismus σ von A auf B. Setze $C := \{a + a^\sigma \mid a \in A\}$. Ist $0 \neq p \in A$, so ist $A = pR$, da A ja irreduzibel ist. Daher ist

$$(p + p^\sigma)R = \bigl\{pr + (pr)^\sigma \mid r \in R\bigr\} = \{a + a^\sigma \mid a \in A\} = C.$$

Somit ist auch C irreduzibel. Ferner gilt $C \neq A$, B und $C \leq A + B$. Folglich ist $A \sim B$.

Es sei umgekehrt $A \sim B$ und C sei ein von A und B verschiedener, irreduzibler Teilmodul in $A + B$. Nun ist $A + B = A \oplus B$. Es gibt daher Projektionen α und β von C in A beziehungsweise B. Weil A, B und C irreduzibel sind und C von A und auch B verschieden ist, sind α und β Isomorphismen. Es folgt, dass $\alpha^{-1}\beta$ ein Isomorphismus von A auf B ist. Somit gilt auch $A \equiv B$, womit die Gleichheit der beiden Äquivalenzrelationen bewiesen ist. Mittels 2.15 und 4.1 folgt nun die Behauptung des Satzes.

Die H_Φ heißen aus offensichtlichem Grund *homogene Komponenten* von M.

Das Rechtsideal I des Ringes R heißt *minimal*, wenn $L_R(I)$ genau zwei Elemente enthält. Man beachte, dass ein minimales Rechtsideal als Rechtsmodul über R nicht notwendig irreduzibel ist, da ja durchaus $IR = \{0\}$ sein kann.

Der Ring R heißt *vollständig reduzibel*, falls er als Rechtsmodul über sich selbst vollständig reduzibel ist. Die Atome eines solchen Ringes sind gerade die minimalen Rechtsideale von R. Ist nämlich I ein minimales Rechtsideal, so gibt es ein Atom, also ein weiteres minimales Rechtsideal P, mit $P \leq I$. Hieraus folgt $P = I$. Es gilt also für alle minimalen Rechtsideale I von R, dass $IR = I$ ist.

4.6. Satz. *Es sei R ein vollständig reduzibler Ring und $I_R(R)/\equiv$ sei die Menge der Äquivalenzklassen isomorpher, minimaler Rechtsideale von R. Ist $\Phi \in I_R(R)/\equiv$, so ist H_Φ ein zweiseitiges Ideal von R. Ferner gilt im ringtheoretischen Sinne*

$$R = \bigoplus_{\Phi \in I_R(R)/\equiv} H_\Phi.$$

Beweis. Als Summe von Rechtsidealen ist H_Φ natürlich auch ein Rechtsideal. Es sei nun I ein minimales Rechtsideal in H_Φ. Ist $0 \neq r \in I$, so ist $I = rR$. Es sei $s \in R$. Wir definieren σ durch $(rk)^\sigma := srk$ für alle $k \in R$. Dann ist σ ein Epimorphismus von I auf srR. Weil I minimal ist, ist daher entweder $srR = \{0\}$ oder srR ist ein zu I isomorphes Rechtsideal von R. In beiden Fällen ist $srR \leq H_\Phi$. Somit sind die homogenen Komponenten von R zweiseitige Ideale.

Sind Φ und Ψ verschiedene Äquivalenzklassen minimaler Rechtsideale, so ist $H_\Phi \cap H_\Psi = \{0\}$ und daher $xy = 0$ für $x \in H_\Phi$ und $Y \in H_\Psi$. Hieraus folgt, dass R auch im ringtheoretischen Sinne die direkte Summe seiner homogenen Komponenten ist. Damit ist alles bewiesen.

Der vollständig reduzible Ring R heißt *homogen*, falls er nur eine homogene Komponente hat. Dies ist gleichbedeutend damit, dass alle minimalen Rechtsideale von R als R-Rechtsmoduln isomorph sind. Ist R einfach, dh., besitzt R nur die beiden zweiseitigen Ideale $\{0\}$ und R, so ist R nach dem gerade bewiesenen Satz homogen. Die Umkehrung gilt nicht, wie wir noch sehen werden.

4.7. Satz. *Ist R ein vollständig reduzibler Ring, und ist M ein R-Rechtsmodul, so ist M genau dann vollständig reduzibel, wenn $MR = M$ ist. Ist $MR = M$ und ist R homogen, so ist $L_R(M)$ irreduzibel.*

Beweis. Es sei M ein R-Rechtsmodul mit $MR = M$. Wir zeigen, dass M Summe von Atomen ist. Dazu sei $0 \neq y \in M$. Wir definieren die Abbildung φ von R auf yR durch $r^\varphi := yr$. Dann sind die Moduln $R/\mathrm{Kern}(\varphi)$ und yR isomorph. Weil $L_R(R)$ ein projektiver Verband ist, ist auch $L_R(R/\mathrm{Kern}(\varphi))$ ein projektiver Verband. Also ist $R/\mathrm{Kern}(\varphi)$ und dann auch yR Summe von Atomen. Folglich ist M wegen $M = MR$ Summe von Atomen, so dass M ein vollständig reduzibler R-Modul ist.

Ist M vollständig reduzibel, so ist M Summe von irreduziblen Teilmoduln. Ist P ein solcher und ist $0 \neq y \in P$, so ist $P = yR$, wie wir wissen. Hieraus folgt, dass $MR = M$ ist.

Es bleibt, die Irreduzibilität von $L_R(M)$ zu beweisen, falls R homogen ist und $MR = M$ gilt. In diesem Falle sind alle minimalen Rechtsideale von R isomorph, da R nur eine homogene Komponente hat. Da ein Atom von M aber stets zu einem minimalen Rechtsideal von R isomorph ist, wie unmittelbar aus 4.2 folgt, sind auch alle Atome von M isomorph, woraus sich die Irreduzibilität von $L_R(M)$ ergibt.

Jeder Körper K, ob kommutativ oder nicht, ist natürlich ein vollständig reduzibler Ring. Daher erhalten wir aufs Neue den Satz, dass $L_K(V)$ ein projektiver Verband ist, falls nur V ein Rechtsvektorraum über K ist. Da K ein einfacher Ring ist, ist $L_K(V)$ auch irreduzibel. Gibt es weitere vollständig reduzible Ringe? Die Antwort lautet: Ja.

Um dies einzusehen, holen wir zunächst etwas weiter aus. Es sei V ein Rechtsvektorraum über dem Körper K. Es sei ferner $\mathrm{End}_K(V)$ der Endomorphismenring von V, wobei wir das Bild des Vektors v unter dem Endomorphismus σ mit $\sigma(v)$ bezeichnen. Schließlich benötigen wir noch die Definition des Begriffs *von Neumann-Ring*. Ein Ring R werde so genannt, falls es zu jedem $r \in R$ ein $s \in R$ gibt mit $rsr = r$. Ist $rsr = r$, so sind die Elemente rs und sr *Idempotente*, dh., es gilt $(rs)^2 = rs$ und $(sr)^2 = sr$, wie man unmittelbar sieht. Die Idempotente eines Endomorphismenringes heißen auch *Projektionen*. Ist R ein von Neumann-Ring, sind r, $s \in R$ und gilt $rsr = r$, so ist $rsR = rR$. Denn einmal ist $rs \in rR$ und andererseits ist $r = (rs)r \in rsR$. Jedes Hauptrechtsideal eines von Neumann-Ringes wird also von einem Idempotenten erzeugt. Hieraus folgt weiter, dass für ein Rechtsideal I von R, welches nicht gleich $\{0\}$ ist, auch I^2 von $\{0\}$ verschieden ist, da jedes derartige Ideal ein von 0 verschiedenes, idempotentes Element enthält. Die gleiche Aussage gilt natürlich auch für Linksideale.

4.8. Satz. *Ist V ein Rechtsvektorraum über dem Körper K, so ist $\mathrm{End}_K(V)$ ein von Neumann-Ring. Genauer: Es sei Y ein Komplement von $\mathrm{Kern}(\varphi)$, wobei φ ein Endomorphismus von V sei. Dann ist $\varphi(V) = \varphi(Y)$ und die Einschränkung von φ auf Y ist ein Monomorphismus. Es sei weiter Z ein Komplement von $\varphi(Y)$. Definiere ψ durch $\psi(z) := 0$ für $z \in Z$ und $\psi(\varphi(y)) := y$ für alle $y \in Y$. Dann ist $\varphi\psi\varphi = \varphi$. Überdies sind die Ränge von φ und ψ gleich.*

Beweis. Es ist klar, dass die Einschränkung von φ auf Y injektiv ist, so dass die Definition von ψ korrekt ist. Es sei nun $v \in V$. Es gibt dann ein $y \in Y$ und ein $k \in \mathrm{Kern}(\varphi)$ mit $v = y + k$. Es folgt

$$\begin{aligned}\varphi\psi\varphi(v) &= \varphi\psi\varphi(y+k) = \varphi\psi\big(\varphi(y)+\varphi(k)\big) = \varphi\big(\psi\varphi(y)\big)\\ &= \varphi(y) = \varphi(y) + \varphi(k) = \varphi(v),\end{aligned}$$

so dass in der Tat $\varphi\psi\varphi = \varphi$ gilt.

Wir ziehen einige Folgerungen aus diesem Satz.

4.9. Satz. *Es sei V ein K-Vektorraum und $J_K(V)$ sei die Menge der Endomorphismen endlichen Ranges von V. Dann ist $J_K(V)$ ein zweiseitiges Ideal von*

$\mathrm{End}_K(V)$. Ferner gilt, dass $J_K(V)$, für sich betrachtet, ein von Neumann-Ring ist.

Beweis. Es ist eine simple Übungsaufgabe zu zeigen, dass $J_K(V)$ ein zweiseitiges Ideal ist. Ist nun $\rho \in J_K(V)$, so gibt es nach 4.8 ein $\sigma \in \mathrm{End}_K(V)$ mit $\rho\sigma\rho = \rho$, so dass die Ränge von ρ und σ gleich sind. Also gilt sogar $\sigma \in J_K(V)$. Damit ist alles bewiesen.

4.10. Satz. *Es sei V ein K-Vektorraum.*
a) *Ist $\varphi \in \mathrm{End}_K(V)$, so gibt es eine Projektion $\pi \in J_K(V)$ mit*

$$\varphi\mathrm{End}_K(V) = \pi\mathrm{End}_K(V).$$

b) *Ist $\varphi \in J_K(V)$, so gibt es eine Projektion $\pi \in J_K(V)$ mit*

$$\varphi J_K(V) = \pi J_K(V).$$

Beweis. Dies folgt aus der Bemerkung, die vor 4.8 gemacht wurde, und der Tatsache, dass die beiden Ringe $\mathrm{End}_K(V)$ und $J_K(V)$ von Neumann-Ringe sind.

4.11. Satz. *Es seien π und ρ Projektionen des K-Vektorraumes V. Ist $\pi(V) = \rho(V)$ und hat $\pi(V)$ den Rang 1, so ist $\pi\mathrm{End}_K(V) = \rho\mathrm{End}_K(V)$ und $\pi\mathrm{End}_K(V)$ ist ein Rechtsideal von $\mathrm{End}_K(V)$, welches minimal ist. Ferner gilt: Ist I ein minimales Ideal von $\mathrm{End}_K(V)$, so gibt es eine Projektion π des Ranges 1 mit $I = \pi\mathrm{End}_K(V)$.*

Beweis. Setze $P := \pi(V)$. Dann ist

$$P \oplus \mathrm{Kern}(\pi) = V = P \oplus \mathrm{Kern}(\rho).$$

Ist $\mathrm{Kern}(\pi) = \mathrm{Kern}(\rho)$, so ist $\pi = \rho$ und die von π und ρ erzeugten Ideale sind gleich. Es sei also $\mathrm{Kern}(\pi) \neq \mathrm{Kern}(\rho)$. Dann ist

$$V = \mathrm{Kern}(\pi) + \mathrm{Kern}(\rho)$$

und daher

$$\begin{aligned}\mathrm{Kern}(\pi)/\big(\mathrm{Kern}(\pi) \cap \mathrm{Kern}(\rho)\big) &\cong \big(\mathrm{Kern}(\pi) + \mathrm{Kern}(\rho)\big)/\mathrm{Kern}(\rho)\\ &= V/\mathrm{Kern}(\rho).\end{aligned}$$

Es gibt also einen Punkt A auf $\mathrm{Kern}(\pi)$ mit

$$\mathrm{Kern}(\pi) = A + \big(\mathrm{Kern}(\pi) \cap \mathrm{Kern}(\rho)\big).$$

Die Gerade $A+P$ ist ein Komplement von $\mathrm{Kern}(\pi) \cap \mathrm{Kern}(\rho)$. Ebenso folgt die Existenz eines Punktes B auf $\mathrm{Kern}(\rho)$ mit

$$\mathrm{Kern}(\rho) = B + \big(\mathrm{Kern}(\pi) \cap \mathrm{Kern}(\rho)\big).$$

Die Gerade $B+P$ ist ebenfalls ein Komplement von $\mathrm{Kern}(\pi) \cap \mathrm{Kern}(\rho)$. Es seien nun a, b und p Vektoren mit $A = aK$, $B = bK$ und $P = pK$. Wir definieren

dann eine lineare Abbildung λ von V in sich durch $\lambda(p) := p$, $\lambda(a) := b$ und $\lambda(u) := u$ für alle $u \in \mathrm{Kern}(\pi) \cap \mathrm{Kern}(\rho)$. Dann ist $\pi = \rho\lambda$ und, da λ offenbar invertierbar ist, $\rho = \pi\lambda^{-1}$, so dass in der Tat $\rho\mathrm{End}_K(V) = \pi\mathrm{End}_K(V)$ ist.

Es sei nun $0 \neq \sigma \in \pi\mathrm{End}_K(V)$. Nach 4.10 dürfen wir annehmen, dass σ eine Projektion ist. Mit dem bereits Bewiesenen folgt, dass $\sigma\mathrm{End}_K(V) = \pi\mathrm{End}_K(V)$ ist. Folglich ist $\pi\mathrm{End}_K(V)$ ein minimales Ideal.

Es sei $0 \neq \pi \in I$. Dann ist $\pi\mathrm{End}_K(V) = I$, da $\mathrm{End}_K(V)$ ja eine Eins hat und I minimal ist. Nach 4.10 dürfen wir annehmen, dass π eine Projektion ist. Es sei $P := \pi(V)$. Ferner sei $P = Q \oplus C$ mit einem Teilraum Q des Ranges 1. Ist dann σ die Projektion von V auf Q, deren Kern gleich $C \oplus \mathrm{Kern}(\pi)$ ist, so ist $\sigma = \pi\sigma$. Weil I minimal und $\sigma \neq 0$ ist, folgt $\sigma\mathrm{End}_K(V) = \pi\mathrm{End}_K(V)$. Es gibt also ein $\gamma \in \mathrm{End}_K(V)$ mit $\pi = \sigma\gamma$. Daher ist

$$P = \pi(V) = \sigma\gamma(V) \leq \sigma(V) = Q,$$

so dass in der Tat $\mathrm{Rg}(P) = 1$ ist.

4.12. Satz. *Es sei V ein Rechtsvektorraum über dem Körper K. Die minimalen Rechtsideale von $\mathrm{End}_K(V)$ sind genau die minimalen Rechtsideale von $J_K(V)$, wobei $J_K(V)$ für sich als Ring betrachtet ist.*

Beweis. Es sei I ein minimales Rechtsideal von $J_K(V)$. Ferner sei $0 \neq \sigma \in I$. Nach 4.10 b) gibt es eine Projektion $\pi \in J_K(V)$ mit $\sigma J_K(V) = \pi J_K(V)$. Es folgt $\pi \neq 0$ und weiter $0 \neq \pi = \pi^2 \in \pi J_K(V)$. Die Minimalität von I erzwingt daher, dass

$$\sigma J_K(V) = \pi J_K(V) = I$$

ist. Da $\mathrm{End}_K(V)$ eine Eins hat und $J_K(V)$ ein Ideal von $\mathrm{End}_K(V)$ ist, gilt

$$J_K(V)\mathrm{End}_K(V) = J_K(V).$$

Also ist

$$I\mathrm{End}_K(V) = \sigma J_K(V)\mathrm{End}_K(V) = \sigma J_K(V) = I,$$

so dass I ein Rechtsideal von $\mathrm{End}_K(V)$ ist. Hieraus folgt schließlich

$$I = \sigma J_K(V) \subseteq \sigma\mathrm{End}_K(V) \subseteq I,$$

so dass I auch ein minimales Ideal von $\mathrm{End}_K(V)$ ist.

Es sei umgekehrt I ein minimales Rechtsideal von $\mathrm{End}_K(V)$. Es gibt dann eine Projektion π vom Range 1 mit $I = \pi\mathrm{End}_K(V)$. Es folgt $\pi \in J_K(V)$ und damit $I \subseteq J_K(V)$. Also ist I ein Rechtsideal von $J_K(V)$. Es sei nun I' ein von $\{0\}$ verschiedenes Rechtsideal von $J_K(V)$, welches in I enthalten ist. Dann enthält I' eine Projektion σ ungleich Null. Dann ist $\sigma J_K(V)$ ein von $\{0\}$ verschiedenes Rechtsideal von $\mathrm{End}_K(V)$, welches in I enthalten ist. Aus der Minimalität von I folgt daher

$$I = \sigma J_K(v) \subseteq I' \subseteq I,$$

so dass $I = I'$ ist. Also ist I auch ein minimales Ideal von $J_K(V)$.

4.13. Satz. *Ist V ein K-Rechtsvektorraum, so ist $J_K(V)$ ein einfacher, vollständig reduzibler Ring.*

Beweis. Wir zeigen zunächst, dass $J_K(V)$ vollständig reduzibel ist. Dazu sei $\sigma \in J_K(V)$. Weil $J_K(V)$ ein von Neumann-Ring ist, gibt es ein $\rho \in J_K(V)$, so dass $\sigma = \sigma\rho\sigma$ ist. Setze $\pi := \sigma\rho$. Dann ist π eine Projektion und $\pi(V)$ hat endlichen Rang. Es gibt also eine Basis $b_1, \ldots, b_n$ von $\pi(V)$. Wir definieren Projektionen $\pi, \ldots, \pi_n$ durch

$$\pi_i(b_j) := \begin{cases} b_i & \text{für } i = j \\ 0 & \text{für } i \neq j \end{cases}$$

und $\pi_i(h) := 0$ für $h \in \mathrm{Kern}(\pi)$. Dann ist $\pi = \sum_{i:=1}^n \pi_i$ und daher

$$\sigma = \pi\sigma = \sum_{i:=1}^n \pi_i\sigma.$$

Hieraus und aus Satz 4.12 folgt, dass $J_K(V)$ Summe von minimalen Idealen ist. Weil die minimalen Ideale Projektionen enthalten, sind sie auch irreduzible $J_K(V)$-Moduln, so dass $J_K(V)$ ein vollständig reduzibler Ring ist.

Als Nächstes zeigen wir, dass $J_K(V)$ homogen ist. Dazu seien I und I' minimale Rechtsideale dieses Ringes. Es gibt dann zwei Punkte P und Q von $L_K(V)$ mit

$$I = \{\sigma \mid \sigma \in J_K(V), \sigma(V) \leq P\}$$

und

$$I' = \{\sigma \mid \sigma \in J_K(V), \sigma(V) \leq Q\}.$$

Ist $P = Q$, so ist $I = I'$ und nichts weiter zu beweisen. Es sei also $P \neq Q$. Es sei C ein Komplement von $P + Q$. Ferner sei $P = pK$ und $Q = qK$ sowie $R := (p+q)K$. Setze $H := R + C$. Dann ist H ein Komplement von P wie auch von Q. Es sei π die Projektion von V auf P mit $\mathrm{Kern}(\pi) = H$ und π' die Projektion von V auf Q mit $\mathrm{Kern}(\pi') = H$. Dann ist $I = \pi J_K(V)$ und $I' = \pi' J_K(V)$. Definiere λ durch $\lambda(p) := q$, $\lambda(q) := p$ und $\lambda(c) := 0$ für alle $c \in C$. Dann ist

$$\lambda\pi\lambda(q) = \lambda\pi(p) = \lambda(p) = q = \pi'(q)$$

und

$$\lambda\pi\lambda(p+q) = \lambda\pi(p+q) = 0 = \pi'(p+q)$$

sowie

$$\lambda\pi\lambda(c) = 0 = \pi'(c)$$

für alle $c \in C$. Weil $p + Q = p + R$ und daher auch $V = (P + R) \oplus C$ gilt, folgt $\pi' = \lambda\pi\lambda$. Ferner ist klar, dass λ in $J_K(V)$ liegt.

Wir definieren nun φ durch $\varphi(\pi\sigma) := \lambda\pi\sigma$. Dann ist φ ein Modulepimorphismus von I auf $\varphi(I)$. Nun ist $\varphi(\pi\lambda) = \lambda\pi\lambda = \pi'$. Weil I und I' minimale Rechtsideale sind, folgt hieraus, dass $\varphi(I) = I'$ ist. Daher ist φ ein Isomorphismus von I auf I'. Damit ist gezeigt, dass $J_K(V)$ homogen ist.

Es sei schließlich N ein von $\{0\}$ verschiedenes, zweiseitiges Ideal von $J_K(V)$. Ferner sei $\pi J_K(V)$ ein minimales Rechtsideal, welches in N enthalten sei, und π sei idempotent. Eine solche Konstellation existiert, da N ja ungleich $\{0\}$ ist. Es sei weiter I ein minimales Rechtsideal von $J_K(V)$. Weil $J_K(V)$ homogen ist, gibt es einen Modulisomorphismus φ von $\pi J_K(V)$ auf I. Setze $\iota := \varphi(\pi)$. Dann ist

$$0 \neq \iota = \varphi(\pi) = \varphi(\pi^2) = \iota\pi \in I \cap N,$$

so dass $I \subseteq N$ gilt. Weil $J_K(V)$ Summe von minimalen Rechtsidealen ist, ist also $J_K(V) \subseteq N$, so dass $J_K(V)$, wie behauptet, einfach ist.

Das zuletzt benutzte Argument wird uns später noch einmal gute Dienste leisten.

Mit den Ringen $J_K(V)$ haben wir nun viele Beispiele von vollständig reduziblen Ringen gewonnen, die in aller Regel keine Körper sind. Diese Ringe haben überdies keine Eins, wenn V nicht endlichen Ranges ist. Hat V endlichen Rang, so ist $J_K(V) = \mathrm{End}_K(V)$, so dass in diesem Falle $\mathrm{End}_K(V)$ ein einfacher, vollständig reduzibler Ring ist. Man kann noch etwas mehr sagen, nämlich:

4.14. Satz. *Es sei V ein K-Rechtsvektorraum. Ist N ein von $\{0\}$ verschiedenes, zweiseitiges Ideal von $\mathrm{End}_K(V)$, so ist $J_K(V) \subseteq N$.*

Beweis. Wie wir wissen, enthält N eine von Null verschiedene Projektion π. Es sei P ein Punkt mit $P \leq \pi(V)$ und ρ sei eine Projektion von V auf P mit $\mathrm{Kern}(\pi) \subseteq \mathrm{Kern}(\rho)$. Ist $v \in V$, so gibt es ein $c \in \pi(V)$ und ein $x \in \mathrm{Kern}(\pi)$ mit $v = c + x$. Es folgt

$$\rho\pi(v) = \rho\big(\pi(c) + \pi(x)\big) = \rho(c) = \rho(c) + \rho(x) = \rho(v).$$

Also ist

$$0 \neq \rho = \rho\pi \in J_K(V) \cap N,$$

dh., $J_K(V) \cap N$ ist ein von $\{0\}$ verschiedenes, zweiseitiges Ideal von $\mathrm{End}_K(V)$. Weil $J_K(V)$ einfach ist, folgt hieraus $J_K(V) \cap N = J_K(V)$, so dass in der Tat $J_K(V) \subseteq N$ gilt.

Es ist natürlich zu fragen, was $L_{J_K(V)}(J_K(V))$ mit $L_K(V)$ zu tun hat. Man erwartet, dass diese beiden Verbände isomorph sind, und die Erwartung trügt nicht, wie der nächste Satz lehrt.

4.15. Satz. *Es sei V ein K-Rechtsvektorraum. Definiert man Φ und Ψ durch*

$$\Phi(U) := \big\{\sigma \mid \sigma \in J_K(V), \sigma(V) \leq U\big\}$$

für alle $U \in L_K(V)$ und

$$\Psi(I) := \textstyle\sum_{\sigma \in I} \sigma(V)$$

für alle Rechtsideale I von $J_K(V)$, so ist Φ ein Isomorphismus von $L_K(V)$ auf $L_{J_K(V)}(J_K(V))$ und es gilt $\Psi = \Phi^{-1}$.

Beweis. Es ist trivial, dass $\Psi(U)$ für alle $U \in L_K(V)$ ein Rechtsideal von $J_K(V)$, und noch banaler, dass $\Psi(I)$ für alle Rechtsideale I von $J_K(V)$ ein Teilraum von V ist.

Ist $U \in L_K(V)$, so gilt

$$\begin{aligned}\Psi\Phi(U) &= \Psi\bigl(\{\sigma \mid \sigma \in J_K(V), \sigma(V) \leq U\}\bigr) \\ &= \sum_{\sigma \in J_K(V), \sigma(V) \leq U} \sigma(V) \ \leq \ U.\end{aligned}$$

Ist P ein Punkt mit $P \leq U$, so gibt es eine Projektion π mit $\pi(V) = P$. Es folgt $P \leq \Psi\Phi(U)$. Weil U die obere Grenze der in U enthaltenen Punkte ist, folgt weiter $\Psi\Phi(U) = U$. Somit ist $\Psi\Phi = id_{L_K(V)}$.

Es sei I ein Rechtsideal von $J_K(V)$. Dann gilt

$$\Phi\Psi(I) = \Phi\biggl(\sum_{\sigma \in I} \sigma(V)\biggr) = \Bigl\{\tau \mid \tau \in J_K(V), \tau(V) \leq \sum_{\sigma \in I} \sigma(V)\Bigr\} \ \leq \ I.$$

Es sei τ eine Projektion von V auf einen Punkt von $\sum_{\sigma \in I} \sigma(V)$. Wir zeigen, dass $\tau \in I$ gilt. Es gibt eine endliche Teilmenge E von I mit

$$\tau(V) \leq \sum_{\sigma \in E} \sigma(V),$$

da τ ja endlichen Rang hat. Zu jedem $\sigma \in E$ gibt es endlich viele minimale Rechtsideale in I, deren Summe σ enthält. Hieraus schließt man, dass es endlich viele Projektionen $\pi_1, \ldots, \pi_n \in I$ gibt, so dass alle π_i den Rang 1 haben und

$$\tau(V) \leq \sum_{i:=1}^{n} \pi_i(V)$$

gilt. Ist $\tau(V) = \pi_1(V)$ — dies ist gewiss dann der Fall, wenn $n = 1$ ist —, so gilt nach 4.12 und 4.11 die Gleichung

$$\tau J_K(V) = \tau \mathrm{End}_K(V) = \pi \mathrm{End}_K(V) = \pi_1 J_K(V),$$

so dass in diesem Falle $\tau \in I$ gilt. Wir dürfen daher annehmen, dass $\tau(V) \neq \pi_1(V)$ gilt.

Es ist $\tau(V) \leq \pi_1(V) + \sum_{i:=2}^{n} \pi_i(V)$. Nach 2.6 gibt es daher eine Projektion σ von V auf einen Punkt von $\sum_{i:=2}^{n} \pi_i(V)$ mit $\tau(V) \leq \pi_1(V) + \sigma(V)$. Nach der nicht explizit formulierten Induktionsannahme ist $\sigma \in I$, so dass wir oBdA annehmen dürfen, dass $\sigma = \pi_2$ ist. Wegen 4.11 dürfen wir weiter annehmen, dass $\pi_1(V) \leq \mathrm{Kern}(\pi_2)$ und $\pi_2(V) \leq \mathrm{Kern}(\pi_1)$ gilt. Dann ist $\mathrm{Kern}(\pi_1) \cap \mathrm{Kern}(\pi_2)$ ein Komplement von $\pi_1(V) + \pi_2(V)$. Es sei ρ die Projektion von V auf $\pi_1(V) + \pi_2(V)$ mit $\mathrm{Kern}(\rho) = \mathrm{Kern}(\pi_1) \cap \mathrm{Kern}(\pi_2)$. Dann ist $\rho\tau(v) = \tau(v)$ für alle $v \in V$ und daher $\rho\tau = \tau$. Ist nun $v \in V$, so gibt es ein $u_1 \in \pi_1(V)$, ein $u_2 \in \pi_2(V)$ und ein $x \in \mathrm{Kern}(\rho)$ mit $v = u_1 + u_2 + x$. Es folgt

$$\rho(v) = \rho(u_1 + u_2 + x) = u_1 + u_2 = \pi_1(v) + \pi_2(v) = (\pi_1 + \pi_2)(v),$$

so dass $\rho = \pi_1 + \pi_2 \in I$ gilt. Es folgt $\tau = \rho\tau \in I$.

Es gilt also, dass alle minimalen Rechtsideale, die in $\Phi\Psi(I)$ enthalten sind, bereits in I liegen. Daher gilt auch $\Phi\Psi(I) \leq I$, so dass $\Phi\Psi(I) = I$ ist. Damit ist gezeigt, dass Φ eine Bijektion und dass Ψ ihre Inverse ist. Da beide Abbildungen offensichtlich inklusionstreu sind, ist alles bewiesen.

Einmalig neugierig geworden, möchte man möglichst alles über vollständig reduzible Ringe wissen. Wir werden daher im übernächsten Abschnitt noch einmal auf sie zu sprechen kommen. Zuvor jedoch wollen wir die Basis unserer Kenntnisse noch verbreitern.

5. Der duale Verband

Es sei $(L, \leq)$ ein Verband. Wir definieren $(L^d, \leq^d)$, indem wir $L^d := L$ setzen und $\leq^d$ dadurch definieren, dass $A \leq^d B$ genau dann gelte, wenn $B \leq A$ gilt. Bezeichnet man die obere Grenze zweier Elemente A und B von L^d mit $A +^d B$ und ihre untere Grenze mit $A \cap^d B$, so ist $A +^d B = A \cap B$ und $A \cap^d B = A + B$. Daher ist auch $(L^d, \leq^d)$ ein Verband. Er heißt der zu $(L, \leq)$ *duale Verband*.

5.1. Satz. *Ist L ein Verband und ist L^d der zu L duale Verband, so gelten die folgenden Aussagen.*
a) *Ist L modular, so ist auch L^d modular.*
b) *Ist L komplementär, so ist auch L^d komplementär.*
c) *Ist L vollständig, so ist auch L^d vollständig.*

Beweis. a) Der Verband L sei modular. Ferner seien A, B, $C \in L^d$ und es gelte $B \leq^d A$. Dann ist also $A \leq B$. Hieraus folgt

$$A \cap^d (B +^d C) = A + (B \cap C) = B \cap (A + C) = B +^d (A \cap^d C),$$

so dass auch L^d modular ist.

b) und c) folgen unmittelbar aus der Definition der Komplementarität, bzw. der Vollständigkeit.

Wichtig ist auch der nächste Satz.

5.2. Satz. *Es sei L ein modularer und komplementärer Verband. Ist L atomar, so ist auch L^d atomar.*

Beweis. Die Atome von L^d sind gerade die Komplemente der Atome von L. Wir nennen sie, wie schon im Fall der projektiven Verbände, *Hyperebenen* von L oder auch *Ko-Atome* von L.

Wir müssen zeigen, dass jedes vom größten Element Π von L verschiedene Element A in einer Hyperebene von L liegt. Weil L komplementär ist, gibt es ein $B \in L$ mit $\Pi = A \oplus B$. Wegen $A \neq \Pi$ ist $B \neq 0$. Es gibt also ein Atom P von L mit $P \leq B$. Nach 2.10 ist L relativ komplementär. Es gibt daher ein C mit $B = P \oplus C$. Setze $K := A + C$. Dann ist $A \leq K$. Ferner gilt

$$P + K = P + A + C = A + B = \Pi.$$

Andererseits ist

$$P \cap K \leq B \cap K = B \cap (C + A) = C + (B \cap A) = C$$

und daher $P \cap K \leq P \cap C = 0$. Folglich ist K ein Ko-Atom von L, welches A umfasst. Damit ist alles bewiesen.

5.3. Korollar. *Ist L ein modularer, komplementärer und atomarer Verband, so ist jedes vom größten Element verschiedene Element von L gleich dem Schnitt der es umfassenden Hyperebenen.*

Beweis. Dies folgt mittels 5.2, 5.1 und 2.11.

Der Verband L heißt *noethersch*, wenn jede nicht leere Teilmenge von L ein maximales Element enthält. Er heißt *artinsch*, wenn jede seiner nicht leeren Teilmengen ein minimales Element enthält.

5.4. Satz. *Ein modularer, komplementärer Verband ist genau dann artinsch, wenn er noethersch ist.*

Beweis. Wegen 5.1 und der Bemerkung, dass $(L^d)^d = L$ ist, genügt es zu zeigen, dass ein modularer und komplementärer Verband artinsch ist, falls er noethersch ist.

Es sei also L ein solcher Verband und M sei eine nicht leere Teilmenge von L. Wir nehmen an, dass M kein minimales Element enthält. Dann gibt es zu jedem $X \in M$ ein $Y \in M$ mit $Y < X$. Auf Grund des Auswahlaxioms gibt es also eine Abbildung f von M in sich mit $f(X) < X$ für alle $X \in M$. Ist nun $Y \in M$, so folgt mittels des dedekindschen Rekursionssatzes die Existenz einer Abbildung g der nicht negativen ganzen Zahlen in M mit $g(0) = Y$ und $g(n{+}1) < g(n)$ für alle n. Weil L nach 2.10 relativ komplementär ist, folgt mittels des Auswahlaxioms die Existenz einer Abbildung c der Menge der natürlichen Zahlen in L mit $g(n) = g(n+1) \oplus c(n+1)$ für alle $n \geq 0$. Setze $W(n) := \sum_{i:=1}^{n} c(i)$. Dann ist

$$W(n) \leq W(n+1)$$

für alle n. Wir zeigen, dass $W(n) \cap g(n) = 0$ ist. Dies ist sicher richtig, falls $n = 1$ ist. Es sei also $n \geq 1$. Dann gilt auf Grund der Induktionsannahme und der Modularität von L, dass

$$W(n+1) \cap g(n+1) \leq \left(\sum_{i:=1}^{n} c(i) + c(n+1) \right) \cap g(n) = c(n+1)$$

ist. Also ist

$$W(n+1) \cap g(n+1) \leq c(n+1) \cap g(n+1) = 0.$$

Weil L noethersch ist, gibt es nun ein N mit $W(N) = W(n)$ für alle $n \geq N$. Hieraus folgt

$$c(N+1) + W(N) = W(N+1) = W(N)$$

und damit $c(N+1) \leq W(N)$. Andererseits ist auch $c(N+1) \leq g(N)$. Folglich gilt $c(N+1) \leq W(N) \cap g(N) = 0$ und damit

$$g(N) = c(N+1) + g(N+1) = g(N+1)$$

im Widerspruch zu $g(N+1) < g(N)$. Also enthält M doch ein minimales Element, so dass L artinsch ist. Damit ist Satz 5.4 bewiesen.

5.5. Satz. *Ein noetherscher, atomarer, komplementärer und modularer Verband ist projektiv.*

Beweis. Es sei L ein solcher Verband. Es ist zu zeigen, dass L vollständig und nach oben stetig ist.

Es sei $M \subseteq L$ und S sei die Menge der unteren Schranken von M. Dann ist S nicht leer, da $0 \in S$ gilt. Weil L noethersch ist, enthält S also ein maximales Element B. Ist $C \in S$, so ist auch $B + C \in S$ und wegen $B \leq B + C$ daher $B = B + C$. Folglich ist $C \leq B$, so dass B das größte Element von S ist. Somit ist $B = \bigcap_{X \in M} X$, so dass L nach 2.1 vollständig ist.

Es sei M ein aufsteigendes System von L. Dann enthält M ein maximales Element G. Weil M aufsteigend ist, folgt $X \leq G$ für alle $X \in M$. Also ist $\sum_{X \in M} X = G$. Es sei nun $Y \in L$. Dann ist

$$Y \cap \sum_{X \in M} X = Y \cap G.$$

Ferner ist $Y \cap X \leq Y \cap G$ für alle $X \in M$. Somit gilt

$$Y \cap G \leq \sum_{X \in M} (Y \cap G) \leq Y \cap G,$$

so dass L auch nach oben stetig ist.

Als Nächstes charakterisieren wir die noetherschen projektiven Verbände als diejenigen projektiven Verbände, deren Rang endlich ist.

5.6. Satz. *Ein projektiver Verband ist genau dann noethersch, wenn er endlichen Rang hat.*

Beweis. Es sei L ein projektiver Verband endlichen Ranges. Ist M eine nicht leere Teilmenge, so gilt nach 3.1, dass $\mathrm{Rg}_L(X) \leq \mathrm{Rg}(L)$ ist für alle $X \in M$. Es gibt daher ein X maximalen Ranges in M. Ist nun $Y \in M$ und gilt $X \leq Y$, so folgt $\mathrm{Rg}_L(Y) \leq \mathrm{Rg}_L(X)$. Hieraus folgt mit 3.1, dass $X = Y$ ist, so dass X maximal ist. Also ist L noethersch.

Es sei umgekehrt L ein noetherscher projektiver Verband. Ist dann M die Menge der endlich erzeugten Teilräume von L, so enthält M ein maximales Element Π. Ist P ein Punkt von L, so ist auch $\Pi + P$ endlich erzeugt und daher $\Pi = \Pi + P$, was $P \leq \Pi$ zur Folge hat. Folglich ist Π das größte Element von L, so dass L endlichen Rang hat.

Wir sind nun in der Lage, die Frage zu beantworten, unter welchen Bedingungen der zu einem projektiven Verband duale Verband projektiv ist. Auf Grund von 2.15 genügt es, diese Frage für irreduzible projektive Verbände zu beantworten. Diese lapidare Feststellung ist nicht so ganz ohne. Sie besagt nämlich, dass L^d genau dann projektiv ist, wenn für jeden irreduziblen Bestandteil I der in 2.15 beschriebenen Zerlegung von L gilt, dass auch I^d projektiv ist. Um dies zu beweisen, muss man auf der Menge der Hyperebenen

von L eine Äquivalenzrelation $\sim$ definieren, so dass neben $H \sim H$ für alle Hyperebenen H gilt, dass für zwei verschiedene Hyperebenen H und H' genau dann $H \sim H'$ gilt, wenn es eine dritte Hyperebene H'' gibt mit $H \cap H' \leq H''$. Dass dies eine Äquivalenzrelation ist, folgt aus 5.1a) und 2.8. Es sei dem Leser überlassen, den Beweis in allen Einzelheiten auszuführen.

5.7. Satz. *Ist L ein irreduzibler projektiver Verband, so ist L^d genau dann projektiv, wenn der Rang von L endlich ist.*

Beweis. L habe endlichen Rang. Dann ist L nach 5.6 noethersch und nach 5.4 dann auch artinsch. Somit ist L^d noethersch. Da L^d nach 5.1 modular und komplementär und nach 5.2 auch atomar ist, ist L^d nach 5.5 auch projektiv.

Es sei L ein projektiver Verband unendlichen Ranges. Ferner sei H eine Hyperebene von L und Φ sei die Menge aller unabhängigen Punktmengen von L, die keinen Punkt von H enthalten. Dann ist Φ von endlichem Charakter und enthält folglich nach dem Lemma von Teichmüller und Tukey ein maximales B. Setze $U := \sum_{P \in B} P$. Wäre $U \cap H < H$, so gäbe es einen Punkt $Q \leq H$ mit $Q \not\leq U \cap H$. Ist $P \in B$, so wäre $P + Q$ eine Gerade, die weder in U noch in H läge. Weil L irreduzibel ist, gäbe es nach 2.14 auf $P + Q$ einen dritten Punkt R, der dann weder in U noch in H läge. Aus der Maximalität von B folgte die Abhängigkeit von $B \cup \{R\}$. Hieraus folgte der Widerspruch $R \leq H$. Also ist doch $U \cap H = H$. Weil U wenigstens einen Punkt enthält, der nicht auf H liegt, ist $U = \Pi$, wobei Π wieder das größte Element von L bezeichne. Somit ist B eine Basis von Π, so dass B insbesondere unendlich ist. Folglich gibt es eine abzählbare Teilmenge $\{P_1, P_2, P_3, \ldots\} \subseteq B$. Setze $H_i := \sum_{j:=i}^{\infty} P_j$. Dann bilden die H_i eine absteigende Kette. Wir zeigen, dass $\bigcap_{i:=i}^{\infty} H_i = 0$ ist. Es seien m und n natürliche Zahlen. Dann gelten die Gleichungen

$$\mathrm{Rg}_L\left(\sum_{k:=1}^{n} P_k\right) = n,$$

$$\mathrm{Rg}_L\left(\sum_{k:=1}^{n+m} P_k\right) = n + m,$$

$$\mathrm{Rg}_L\left(\sum_{k:=n+1}^{n+m} P_k\right) = m.$$

Mittels der Rangformel folgt hieraus, dass

$$\left(\sum_{k:=1}^{n} P_k\right) \cap \left(\sum_{k:=n+1}^{n+m} P_k\right) = 0$$

ist. Der Satz von der endlichen Abhängigkeit, der ja eine Folge der Stetigkeit nach oben ist, liefert dann, dass

$$\left(\sum_{k:=1}^{n} P_k\right) \cap H_{n+1} = 0$$

ist. Hieraus folgt wiederum, dass

$$\bigcap_{i=1}^{\infty} H_i = 0$$

gilt. Wäre nämlich W ein Punkt in diesem Schnitt, so läge W in H_1. Es gäbe dann $P_1, \ldots, P_n$ mit $W \leq \sum_{k:=1}^n P_k$, woraus der Widerspruch $W \leq (\sum_{k:=1}^n P_k) \cap H_{n+1} = 0$ folgte.

Wäre nun L^d projektiv, so wäre L^d nach oben stetig. Folglich wäre

$$H = H + \bigcap_{i:=1}^{\infty} H_i = \bigcap_{i:=1}^{\infty} (H + H_i) = \Pi.$$

Dieser Widerspruch zeigt, dass L^d nicht projektiv ist, falls L nicht endlichen Ranges ist.

Ist N eine maximale Kette aus Elementen des Verbandes L, so nennen wir N ein *Nest* von L. Jedes Nest von L enthält natürlich das größte und das kleinste Element von L, falls L solche Elemente besitzt. Enthält das Nest N von L nur endlich viele Elemente, so nennen wir $|N| - 1$ die *Länge* des Nestes.

5.8. Satz. *Ist L ein projektiver Verband, so sind die folgenden Bedingungen äquivalent:*
a) *Der Rang von L ist endlich.*
b) *Jedes Nest von L hat endliche Länge.*
c) *Es gibt ein Nest endlicher Länge von L.*
Ist $\mathrm{Rg}(L)$ *endlich, so ist die Länge eines jeden Nestes von L gleich* $\mathrm{Rg}(L)$.

Beweis. a) impliziert b). Gilt $\mathrm{Rg}(L) \leq 1$, so ist L das einzige Nest von L, so dass b) und auch der Nachsatz in diesem Falle korrekt ist. Es sei also $\mathrm{Rg}(L) \geq 2$ und N sei ein Nest von L. Es sei M die Menge der von 0 verschiedenen Elemente in N. Weil der Rang von L endlich ist, ist L artinsch, so dass M ein minimales Element X enthält. Ist nun P ein Punkt auf X, so gilt $0 < P \leq X$. Weil N eine maximale Kette ist, ist daher $X = P$. Es ist folglich $\mathrm{Rg}(\Pi/X) = \mathrm{Rg}(L) - 1$. Weil M ein Nest des Quotienten Π/X ist, ist M also endlich und es gilt, dass $\mathrm{Rg}(L) - 1$ die Länge von M ist. Also ist auch N endlich und $\mathrm{Rg}(L)$ ist die Länge von N. Damit ist b) aus a) hergeleitet und auch der Nachsatz vollständig bewiesen.

b) impliziert c). Auf Grund des hausdorffschen Maximumprinzips besitzt L ein Nest. Dieses hat dann nach b) endliche Länge.

c) impliziert a). Es sei N ein Nest endlicher Länge von L. Enthält N höchstens zwei Elemente, so ist $N = L$ und daher $\mathrm{Rg}(L) \leq 1$. Wir dürfen daher annehmen, dass N ein von 0 und Π verschiedenes Element X enthalte. Dann ist

$$N_1 := \{Y \mid Y \in N,\ Y \leq X\}$$

ein Nest von $X/0$ und

$$N_2 := \{Z \mid Z \in N,\ X \leq Z\}$$

ein Nest von Π/X. Weil diese beiden Nester kürzere Länge als N haben, folgt mittels Induktion, dass $X/0$ und Π/X endlichen Rang haben. Daher hat auch L endlichen Rang.

Damit ist alles bewiesen.

5.9. Satz. *Ist L ein irreduzibler projektiver Verband endlichen Ranges, so ist auch L^d ein irreduzibler Verband endlichen Ranges und es gilt $\mathrm{Rg}(L) = \mathrm{Rg}(L^d)$.*

Beweis. Der Verband L^d ist nach 5.7 projektiv. Weil 0 und Π die einzigen Elemente von L sind, die genau ein Komplement haben, haben sie auch als Elemente von L^d genau ein Komplement, so dass auch L^d irreduzibel ist. Weil jedes Nest von L auch ein Nest von L^d ist, hat L^d nach 5.8 ebenfalls endlichen Rang und es gilt $\mathrm{Rg}(L) = \mathrm{Rg}(L^d)$.

5.10. Satz. *Es sei L ein irreduzibler projektiver Verband endlichen Ranges. Ist dann $X \in L$, so gilt*

$$\mathrm{Rg}_L(X) + \mathrm{Rg}_{L^d}(X) = \mathrm{Rg}(L).$$

Der Beweis sei dem Leser als Übungsaufgabe überlassen. Eine Beweisidee findet sich im Beweise von 5.8.

Ist L ein projektiver Verband, ist $X \in L$ und ist der Rang des Quotienten Π/X endlich, so setzen wir $\mathrm{KoRg}_\Pi(X) := \mathrm{Rg}(\Pi/X)$. Wir nennen diese Zahl *Ko-Rang* von X in Π.

5.11. Satz. *Es sei L ein irreduzibler projektiver Verband. Ist $X \in L$, so hat X genau dann endlichen Ko-Rang, wenn X Schnitt von endlichen vielen Hyperebenen ist. Ist $\mathrm{KoRg}_\Pi(X)$ endlich, so ist X Schnitt von $\mathrm{KoRg}_\Pi(X)$ Hyperebenen, jedoch nicht Schnitt von weniger als $\mathrm{KoRg}_\Pi(X)$ Hyperebenen.*

Beweis. Es sei X Schnitt von endlich vielen Hyperebenen und $H_1, \ldots, H_n$ sei eine minimale Menge von Hyperebenen, deren Schnitt X sei. Wegen der Minimalität von n ist dann $H_i \cap H_n$ für $i := 1, \ldots, n-1$ eine Hyperebene in H_n. Ferner ist

$$X = \bigcap_{i:=1}^{n-1} (H_i \cap H_n).$$

Mittels Induktion folgt $\mathrm{KoRg}_{H_n}(X) = n - 1$ und damit dann

$$\mathrm{KoRg}_\Pi(X) = n.$$

Es sei umgekehrt der Ko-Rang von X in Π endlich. Dann ist Π/X ein endlich erzeugter projektiver Verband, der nach Satz 2.14 auch irreduzibel ist, so dass auch $(\Pi/X)^d$ ein endlich erzeugter projektiver Verband ist. Daher ist X Schnitt von endlich vielen Hyperebenen.

Die letzte Aussage des Satzes folgt schließlich daraus, dass der Ko-Rang von X in Π gerade der Rang von $(\Pi/X)^d$ ist.

5.12. Satz. *Es sei L ein irreduzibler projektiver Verband. Haben X, $Y \in L$ beide endlichen Ko-Rang in Π, so haben auch $X+Y$ und $X \cap Y$ endlichen Ko-Rang in Π und es gilt*

$$\mathrm{KoRg}_\Pi(X) + \mathrm{KoRg}_\Pi(Y) = \mathrm{KoRg}_\Pi(X+Y) + \mathrm{KoRg}_\Pi(X \cap Y).$$

Beweis. Weil X und Y Schnitte von endlich vielen Hyperebenen sind, ist auch $X \cap Y$ Schnitt von endlich vielen Hyperebenen. Die Ko-Rangformel ist daher nichts anderes als die Rangformel für $\bigl(\Pi/(X \cap Y)\bigr)^d$.

Ist V ein Rechtsvektorraum über dem Körper K, so ist $L_K(V)$ ein projektiver Verband, wie wir wissen. Hat V endlichen Rang, so hat auch $L_K(V)$ endlichen Rang und $L_K(V)^d$ ist ebenfalls ein projektiver Verband des gleichen Ranges. Es ist richtig, wie wir sehen werden, dass dieser Verband zum Teilraumverband des zu V dualen Vektorraumes isomorph ist. Da die Dualitätstheorie in vielen Büchern der linearen Algebra miserabel dargestellt wird, erläutern wir sie hier noch einmal. Dabei werden dann gleich auch die entsprechenden Notationen für später fixiert. — Viele Bücher der linearen Algebra handeln nur von Vektorräumen über kommutativen Körpern und unterscheiden nicht zwischen Links- und Rechtsvektorräumen, was im Falle von nicht kommutativen Körpern zwingend erforderlich ist. Ihre Autoren glauben, didaktisch geschickt vorzugehen. In Wirklichkeit aber erweisen sie ihren Lesern einen Bärendienst, da die Realität viele ihrer Leser irgendwann einholt, und diese dann oft erhebliche Verständnisschwierigkeiten haben. Hinzu kommt, dass diese Autoren häufig auch noch sagen, sie beschränkten sich auf den Fall kommutativer Körper, im Falle nicht kommutativer Körper ginge eh alles genauso. Dabei ist z. B. das Transponieren im Ring aller $(n \times n)$-Matrizen über einem Körper K genau dann ein Antiautomorphismus dieses Ringes, wenn K kommutativ ist. Es geht also nicht alles genauso.

Es sei V ein K-Rechtsvektorraum. Ist σ ein Homomorphismus von V in einem weiteren K-Vektorraum, so bezeichnen wir das Bild von $v \in V$ unter σ mit σv. Mit V^* bezeichnen wir die Menge aller linearen Abbildungen von V in K. Dann ist V^* mit der punktweise definierten Addition als Verknüpfung eine abelsche Gruppe. Ist $f \in V^*$ und $k \in K$, so definieren wir kf durch $(kf)v := k(fv)$ für alle $v \in V$. Auf diese Weise wird V^* zu einem K-Linksvektorraum, dem *Dualraum* von V.

5.13. Satz. *Es sei V ein K-Rechtsvektorraum und B sei eine Basis von V. Zu jedem $b \in B$ definieren wir $b^* \in V^*$ durch die Vorschrift*

$$b^*c := \begin{cases} 1 & \text{für } c = b \\ 0 & \text{für } c \neq b. \end{cases}$$

Dann ist die Menge

$$B^* := \{b^* \mid b \in B\}$$

linear unabhängig.

Beweis. Es sei E eine endliche Teilmenge von B und k sei eine Abbildung von E in K mit $0 = \sum_{b \in E} k_b b^*$. Ist dann $c \in E$, so folgt

$$0 = 0c = \sum_{b \in E} k_b b^* c = k_c.$$

Somit sind alle endlichen Teilmengen von B^* linear unabhängig und damit auch B^*.

Zur Notation sei noch gesagt, dass wir bei Linksvektorräumen und Linksmoduln $\mathrm{Rg}^K(X)$, $L^K(V)$, $\mathrm{End}^R(M)$ etc. schreiben.

5.14. Satz. *Es sei V ein Rechtsvektorraum über dem Körper K und B sei eine Basis von V. Genau dann ist B^* eine Basis von V^*, wenn der Rang von V endlich ist. Ist der Rang von V endlich, so ist* $\mathrm{Rg}_K(V) = \mathrm{Rg}^K(V^*)$.

Beweis. Der Rang von V sei endlich. Ist $f \in V^*$ und $v \in V$, so gibt es eine Abbildung k von B in K mit $v = \sum_{b \in B} bk_b$. Es folgt

$$\begin{aligned} fv &= f\left(\sum_{b \in B} bk_b\right) = \sum_{b \in B} fbk_b \\ &= \sum_{b \in B} \sum_{c \in B} (fc)c^* bk_b = \sum_{c \in B} \sum_{b \in B} (fc)c^* bk_b \\ &= \left(\sum_{c \in B} (fc)c^*\right) \sum_{b \in B} bk_b = \left(\sum_{c \in B} (fc)c^*\right) v. \end{aligned}$$

Hieraus folgt, dass $f = \sum_{c \in B} (fc)c^*$. Damit ist gezeigt, dass B^* ein Erzeugendensystem von V^* ist. Weil B^* nach 5.13 auch linear unabhängig ist, ist B^* in der Tat eine Basis von V^*. Ferner folgt, dass die Ränge von V und V^* gleich sind. Die Basis B^* heißt die zu B *duale Basis* von V^*.

Der Rang von V sei nun nicht endlich. Wir definieren $f \in V^*$ durch $fb := 1$ für alle $b \in B$. Wäre f ein Element von $\sum_{b \in B} Kb^*$, so gäbe es eine Abbildung k von B in K mit endlichem Träger und $f = \sum_{b \in B} k_b b^*$. Weil der Träger von f endlich, die Menge B aber unendlich ist, gäbe es ein $c \in B$ mit $k_c = 0$. Hieraus folgte der Widerspruch

$$1 = fc = \sum_{b \in B} k_b b^* c = k_c = 0,$$

so dass B^* kein Erzeugendensystem von V^* ist.

Ist V ein Linksvektorraum über dem Körper K, so definiert man ganz entsprechend wie im Falle der Rechtsvektorräume den Dualraum von V. Der Dualraum von V ist dann ein Rechtsvektorraum über K. Die bislang bewiesenen Sätze behalten natürlich *mutatis mutandis* ihre Gültigkeit. Ist V ein Rechtsvektorraum, so bezeichnen wir mit V^{**} den Dualraum von V^*. Der Raum V^{**} ist dann wieder ein Rechtsvektorraum über K. Man nennt ihn den zu V *bidualen Raum*. Der nächste Satz beschreibt den Zusammenhang zwischen V und seinem Bidualen.

5.15. Satz. *Es sei V ein Rechtsvektorraum über dem Körper K. Definiert man für $v \in V$ die Abbildung v^φ von V^* in K vermöge $fv^\varphi := fv$ für alle $f \in V^*$, so ist φ ein Monomorphismus von V in V^{**}. Genau dann ist φ surjektiv, wenn der Rang von V endlich ist.*

Beweis. Routinerechnungen zeigen, dass φ ein Homomorphismus von V in V^{**} ist. Es bleibt zu zeigen, dass φ injektiv ist. Dazu sei $0 \neq v \in V$. Es gibt dann eine Hyperebene H mit $V = vK \oplus H$. Definiere $f \in V^*$ durch $fv := 1$ und $fh := 0$ für alle $h \in H$. Es folgt $1 = fv = fv^\varphi$, so dass $v^\varphi \neq 0$ ist. Somit ist $\mathrm{Kern}(\varphi) = \{0\}$.

Ist V endlichen Ranges, so folgt mit 5.14, dass

$$\mathrm{Rg}_K(V) = \mathrm{Rg}^K(V^*) = \mathrm{Rg}_K(V^{**})$$

ist. Hieraus folgt mittels 3.1, dass $V^\varphi = V^{**}$ ist. In diesem Falle ist φ surjektiv, wie behauptet.

Es sei V nicht endlichen Ranges und B sei eine Basis von V. Nach 5.14 und 5.13 ist $U := \sum_{b \in B} Kb^*$ ein echter Teilraum von V^*. Es sei $f \in V^* - U$. Weil natürlich auch $L^K(V^*)$ ein projektiver Verband ist, gibt es eine Hyperebene H mit $f \notin H$ und $U \leq H$. Es gibt daher ein $g \in V^**$ mit $fg = 1$ und $\mathrm{Kern}(g) = H$. Wäre nun $g = v^\varphi$ mit einem $v \in V$, so wäre

$$0 = b^*g = b^*v^\varphi = b^*v$$

für alle $b \in B$. Nun wäre aber $v = \sum_{c \in B} ck_c$. Wendete man hierauf die Abbildung b^* an, so folgte $0 = k_b$, so dass $v = 0$ wäre im Widerspruch zu $g \neq 0$. Damit ist alles bewiesen.

Ist der Rang von V nicht endlich, so besteht eine Unsymmetrie zwischen V und V^*. Um diese Unsymmetrie zu beseitigen, studieren wir nach dem Vorgange von Artin eine etwas allgemeinere Situation, in der, da sie allgemeiner ist, nicht mehr alle Sätze gelten, die für V und V^* richtig sind. Diesen Nachteil nehmen wir jedoch in Kauf, da er durch den Gewinn der Symmetrie fast wett gemacht wird. Diese Situation wird wie folgt beschrieben. Es sei K ein Körper und W sei ein Links- sowie V ein Rechtsvektorraum über K. Ferner sei f eine Abbildung des cartesischen Produktes von W mit V in K. Das Bild von (w, v) unter f werde mit wv bezeichnet. Wir sagen, dass W mit V *gekoppelt* sei, bzw. dass (W, V, f) ein *duales Raumpaar* bez. des *Skalarproduktes* f sei, falls gilt:

1) Es ist $(w + w')v = wv + w'v$ für alle w, $w' \in W$ und alle $v \in V$.
2) Es ist $w(v + v') = wv + wv'$ für alle $w \in W$ und alle v, $v' \in V$.
3) Es ist $(kw)v = k(wv)$ für alle $k \in K$, alle $w \in W$ und alle $v \in V$.
4) Es ist $w(vk) = (wv)k$ für alle $k \in K$, alle $w \in W$ und alle $v \in V$.
5) Ist $w \in W$ und $wV = \{0\}$, so ist $w = 0$.
6) Ist $v \in V$ und $Wv = \{0\}$, so ist $v = 0$.

Für $X \in L_K(V)$ setzen wir

$$X^\perp := \{w \mid w \in W, wX = \{0\}\}$$

und für $Y \in L^K(W)$ setzen wir

$$y^{\perp} := \{v \mid v \in V, Yv = \{0\}\}.$$

Sind X, $Y \in L_K(V)$ und gilt $X \leq Y$, so gilt $Y^{\perp} \leq X^{\perp}$. Ferner gilt $X \leq X^{\perp\top}$. Sind X, $Y \in L^K(W)$ und gilt $X \leq Y$, so gilt $Y^{\top} \leq X^{\top}$ wie auch $X \leq X^{\top\perp}$. Dies folgt unmittelbar aus den Definitionen.

5.16. Satz. *Es sei K ein Körper, W sei ein K-Links- und V ein K-Rechtsvektorraum. Überdies seien W und V gekoppelt. Ist $X \in L_K(V)$ und $Y \in L^K(W)$, so gilt:*

a) *Es gibt genau einen Monomorphismus φ von $X^{\perp}$ in $(V/X)^*$ mit*

$$y^{\varphi}(v + X) = yv$$

für alle $y \in X^{\perp}$ und alle $v \in V$.

a′) *Es gibt genau einen Monomorphismus ψ von $Y^{\top}$ in $(W/Y)^*$ mit*

$$(w + Y)x^{\varphi} = wx$$

für alle $w \in W$ und alle $x \in Y^{\top}$.

b) *Ist $w \in W$, so definieren wir w^{ζ} durch $w^{\zeta} := wx$ für alle $x \in X$. Dann ist ζ ein Homomorphismus von W in X^* und es gilt* $\mathrm{Kern}(\zeta) = X^{\perp}$. *Ist der Rang von X endlich, so ist ζ surjektiv.*

b′) *Ist $v \in V$, so definieren wir v^{ξ} durch $yv^{\xi} := yv$ für alle $y \in Y$. Dann ist ξ ein Homomorphismus von V in Y^* und es gilt* $\mathrm{Kern}(\xi) = y^{\top}$. *Ist der Rang von Y endlich, so ist ξ surjektiv.*

Beweis. Aus Symmetriegründen genügt es, a) und b) zu beweisen.

a) Ist $y \in X^{\perp}$ und $v + X = v' + X$, so folgt $yv = yv'$. Definiert man daher, y^{φ} durch $y^{\varphi}(v + X) := yv$, so ist y^{φ} wohldefiniert. Es folgt, dass φ eine Abbildung von $X^{\perp}$ in $(V/X)^*$ ist. Triviale Rechnungen zeigen, dass φ sogar ein Homomorphismus ist. Es sei $y^{\varphi} = 0$. Dann ist $yV = \{0\}$ und daher $y = 0$, so dass φ ein Monomorphismus ist.

b) Ist $w \in W$, so definieren wir w^{ζ} durch $w^{\zeta}x := wx$ für alle $x \in X$. Triviale Rechnungen zeigen, dass ζ ein Homomorphismus von W in X^* ist. Ist $w^{\zeta} = 0$, so ist $wX = \{0\}$, so dass $w \in X^{\perp}$ gilt.

Der Rang von X sei endlich. Dann ist nach dem gerade Bewiesenen

$$\mathrm{Rg}^K(W/X^{\perp}) \leq \mathrm{Rg}^K(X^*) = \mathrm{Rg}_K(X).$$

Nach a′) gibt es einen Monomorphismus von $X^{\perp\top}$ in $(W/X^{\perp})^*$. Weil $X \leq X^{\perp\top}$ gilt, ist also

$$\mathrm{Rg}_K(X) \leq \mathrm{Rg}_K(X^{\perp\top}) \leq \mathrm{Rg}_K(W/X^{\perp})^* \leq \mathrm{Rg}_K(X).$$

Somit ist $X = X^{\perp\top}$. Es folgt weiter, dass $\mathrm{Rg}^K(W/X^{\perp}) = \mathrm{Rg}^K(X^*)$ ist. Folglich ist ζ in diesem Falle auch surjektiv.

Damit ist alles bewiesen.

Im Beweise von 5.16 haben wir mehr bewiesen als im Satz formuliert. Darauf werden wir gleich zurückkommen. Zuvor zeigen wir jedoch, dass die Theorie der gekoppelten Räume im Falle von Räumen endlichen Ranges nichts Neues liefert.

5.17. Satz. *Es sei K ein Körper, W sei ein K-Links- und V ein K-Rechtsvektorraum. Überdies seien W und V gekoppelt. Genau dann hat V endlichen Rang, wenn W endlichen Rang hat. Hat einer der beiden Räume endlichen Rang, so haben also beide endlichen Rang und es gilt:*

a) *Ist $w \in W$ und definiert man w^ζ durch $w^\zeta v := wv$ für alle $v \in V$, so ist ζ ein Isomorphismus von W auf V^*.*

b) *Ist $v \in V$ und definiert man v^ξ durch $wv^\xi := wv$ für alle $w \in W$, so ist ξ ein Isomorphismus von V auf W^*.*

Beweis. Es sei V endlichen Ranges. Dann folgt mit 5.16 b), dass ζ ein Epimorphismus von W auf V^* ist und dass $\mathrm{Kern}(\zeta) = V^\perp = \{0\}$ gilt. Also hat auch W endlichen Rang und es gilt a).

Hat W endlichen Rang, so folgt mit 5.16 b$'$), dass V endlichen Rang hat und dass b) gilt. Damit ist alles bewiesen.

5.18. Satz. *Es sei K ein Körper und W und V seien gekoppelte Vektorräume über K. Dann gilt:*

a) *Sind $X, Y \in L_K(V)$ und gilt $X \leq Y$, so ist $Y^\perp \leq X^\perp$.*

b) *Sind $X, Y \in L^K(W)$ und gilt $X \leq Y$, so ist $Y^\top \leq X^\top$.*

c) *Es ist $X \leq X^{\perp\top}$ für alle $X \in L_K(V)$. Hat X endlichen Rang, so gilt $X = X^{\perp\top}$.*

d) *Es ist $X \leq X^{\top\perp}$ für alle $X \in L^K(W)$. Hat X endlichen Rang, so gilt $X = X^{\top\perp}$.*

e) *Es ist $X^{\perp\top\perp} = X^\perp$ für alle $X \in L_K(V)$.*

f) *Es ist $X^{\top\perp\top} = X^\top$ für alle $X \in L^K(W)$.*

Beweis. a), b), c) und d) sind entweder schon als trivial erkannt oder bereits bewiesen, nämlich beim Beweise von 5.16. Es bleiben e) und f) zu beweisen.

Es sei $U \in L_K(V)$. Dann ist $U \leq U^{\perp\top}$ nach c) und folglich $U^{\perp\top\perp} \leq U^\perp$ nach a). Andererseits ist $U^\perp \in L^K(W)$, so dass nach d) gilt, dass $U^\perp \leq U^{\perp\top\perp}$ ist. Damit ist e) bewiesen. Die Aussage f) beweist sich analog.

Das Paar $(\perp, \top)$ ist eine *Galoisverbindung* von $L_K(V)$ mit $L^K(W)$.

5.19. Satz. *Ist V ein Rechtsvektorraum endlichen Ranges über dem Körper K und ist V^* der Dualraum von V, so sind V^* und V gekoppelt und $\perp$ ist ein Isomorphismus des Verbandes $(L_K(V)^d, \leq^d)$ auf den Verband $(L^K(V^*), \leq)$.*

Beweis. Nach 5.18 a) und b) ist $\perp$ eine ordnungserhaltende Abbildung von $(L_K(V)^d, \leq^d)$ in $(L^K(V^*), \leq)$ und $\top$ ist eine ordnungserhaltende Abbildung von $(L^K(V^*), \leq)$ in $(L_K(V)^d, \leq^d)$. Nach 5.18 c) ist ferner $\perp\top$ die Identität auf $L_K(V)$. Weil der Rang von V endlich ist, ist es auch der Rang von V^*. Daher folgt mit 5.18 d), dass $\top\perp$ die Identität auf $L^K(V^*)$ ist. Also ist $\perp$ bijektiv, wie behauptet.

Mit diesem Satz haben wir eine Beschreibung von $L_K(V)^d$ gewonnen, die diesen Verband der Behandlung mittels Methoden der linearen Algebra zugänglich macht. Puristen — und in diesem Zusammenhang sind wir Puristen — werden bemängeln, dass der duale Verband mit Hilfe eines Linksvektorraumes dargestellt wird. Man wünscht sich auch für ihn eine Beschreibung durch einen Rechtsvektorraum. Eine solche Beschreibung ist nun rasch gefunden. Es sei K ein Körper. Wir definieren auf K eine Multiplikation $\circ$ durch $a \circ b := ba$ für alle $a, b \in K$. Dann ist auch $(K, +, \circ)$ ein Körper und die Identität ist ein Antiisomorphismus von K auf jenen Körper, den wir mit $K_\circ$ bezeichnen. Ist nun V ein Linksvektorraum über K, so wird V zu einen Rechtsvektorraum über $K_\circ$ durch die Vorschrift $v \circ a := av$. Offenbar gilt $L^K(V) = L_{K_\circ}(V)$. Wendet man dies nun auf die obige Situation an, so erhält man in $L_{K_\circ}(V^*)$ eine Beschreibung von $L_K(V)^d$ durch einen Rechtsvektorraum über dem zu K antiisomorphen Körper $K_\circ$. Ist K kommutativ, so ist K natürlich gleich $K_\circ$. Daher sind in diesem Falle auch $L_K(V)$ und $L_K(V)^d$ gleich. Im allgemeinen ist dies jedoch nicht der Fall. Mehr darüber im nächsten Kapitel.

Eine interessante Folgerung aus 5.19 ist der nächste Satz.

5.20. Satz. *Es sei V ein Vektorraum endlichen Ranges über dem Körper K. Ist $U \in L_K(V)$, so ist*

$$\mathrm{Rg}_K(V) = \mathrm{Rg}_K(U) + \mathrm{Rg}^K(U^\perp).$$

Dabei ist $\perp$ als Abbildung von $L_K(V)$ in $L^K(V^*)$ aufzufassen.

Beweis. Weil $\perp$ nach 5.19 ein Isomorphismus von $L_K(V)^d$ auf $L^K(V^*)$ ist, ist $\mathrm{KoRg}_K(U) = \mathrm{Rg}^K(U^\perp)$. Hieraus folgt die Behauptung.

5.21. Satz. *Es sei K ein Körper und W und V seien gekoppelte Vektorräume über K. Es sei Ξ die Menge aller Unterräume der Form $X^\perp$ von W, wobei X ein Teilraum endlichen Ranges von V ist. Dann gilt:*

a) *Ist $Y \in \Xi$ und ist Z ein Teilraum von W mit $Y \leq Z$, so ist $Z \in \Xi$.*

b) *Sind Y, $Z \in \Xi$, so ist $Y \cap Z \in \Xi$.*

Entsprechendes gilt, wenn man die Rollen von W und V vertauscht.

Beweis. a) Es gibt ein X endlichen Ranges in $L_K(V)$ mit $Y = X^\perp$. Wir definieren eine Koppelung, der wir diesmal einen Namen, nämlich π, geben, von W/Y mit X durch $(w + Y)x := wx$ für alle $w \in W$ und alle $x \in X$. Wegen $Y = X^\perp$ ist π wohldefiniert. Wir zeigen, dass π eine Koppelung ist. Dazu sind nur die Eigenschaften 5) und 6) nachzuweisen, da die übrigen sich von selbst verstehen. Es sei $(w + Y)X = \{0\}$. Dann ist $wX = \{0\}$ und daher $w \in X^\perp = Y$. Ist $x \in X$ und $(W/Y)x = \{0\}$, so ist $Wx = \{0\}$ und daher $x = 0$. Somit ist π tatsächlich eine Koppelung. Die durch π definierten Abbildungen von Unterräumen des einen Raumes auf ihren annullierenden Unterraum des anderen bezeichnen wir mit $\perp(\pi)$ bzw. $\top(\pi)$.

Es sei nun Z/Y ein Teilraum von W/Y. Dann ist

$$\begin{aligned}(Z/Y)^{\top(\pi)} &= \big\{x \mid x \in X,\ (Z/Y)x = \{0\}\big\}\\ &= \big\{x \mid x \in X,\ Zx = \{0\}\big\}\\ &= Z^\top.\end{aligned}$$

Es sei andererseits U ein Teilraum von X. Dann ist

$$\begin{aligned} U^{\perp(\pi)} &= \{w + Y \mid w \in W,\ (w + Y)U = \{0\}\} \\ &= \{w + Y \mid w \in W,\ wU = \{0\}\} \\ &= U^{\perp}/Y. \end{aligned}$$

Weil X endlichen Rang hat, sind die Abbildungen $\perp(\pi)$ und $\top(\pi)$ Bijektionen. Daher gilt

$$Z/Y = (Z/Y)^{\top(\pi)\perp(\pi)} = (Z^{\top})^{\perp(\pi)} = Z^{\top\perp}/Y.$$

Hieraus folgt

$$Z = Z^{\top\perp}$$

für alle Teilräume Z von W, die Y umfassen. Weil X endlichen Rang hat, gilt aber auch $X = X^{\perp\top}$. Somit ist die Einschränkung von $\perp$ auf $L_K(X)$ eine Bijektion dieser Menge auf die Menge der Teilräume von W, die Y enthalten. Daher gilt a).

b) Es gibt Unterräume A und B endlichen Ranges von V mit $Y = A^{\perp}$ und $Z = B^{\perp}$. Nun ist aber

$$Y \cap Z = A^{\perp} \cap B^{\perp} = (A + B)^{\perp}.$$

Weil auch $A + B$ endlichen Rang hat, ist demnach $Y \cap Z \in \Xi$.

Die nächsten vier Sätze formulieren wir nur für den Fall eines Rechtsvektorraumes und seines Dualraums. Jegliche Verallgemeinerung würde technisch aufwendig und wäre nur schwer zu merken. Falls der Leser allgemeinere Situationen antrifft, wird es ihm nicht schwer fallen, die entsprechenden Sätze aus den hier wiedergegebenen herauszupräparieren.

Ist V ein Linksvektorraum über K und ist σ eine lineare Abbildung von V in einen weiteren K-Linksvektorraum, so bezeichnen wir das Bild von $v \in V$ unter σ mit $v\sigma$.

5.22. Satz. *Es seien V und W Rechtsvektorräume über dem Körper K und V^* und W^* seien ihre Dualräume. Ist $\varphi \in \mathrm{Hom}_K(V, W)$, so gibt es genau ein $\varphi^* \in \mathrm{Hom}^K(W^*, V^*)$ mit $(f\varphi^*)v = f(\varphi v)$ für alle $v \in V$ und alle $f \in W^*$. Die Abbildung $*$ ist ein Monomorphismus von $\mathrm{Hom}_K(V, W)$ in $\mathrm{Hom}^K(W^*, V^*)$. Haben V und W beide endlichen Rang, so ist $*$ ein Isomorphismus der abelschen Gruppe $\mathrm{Hom}_K(V, W)$ auf $\mathrm{Hom}^K(W^*, V^*)$. Ist V endlichen Ranges und gilt $V = W$, so ist $*$ ein Ringisomorphismus von $\mathrm{End}_K(V)$ auf $\mathrm{End}^K(V^*)$.*

Der Beweis dieses Satzes sei dem Leser als Übungsaufgabe überlassen. Man nennt φ^* die zu φ *duale Abbildung*.

5.23. Satz. *Es seien V und W Rechtsvektorräume über dem Körper K. Ist $\varphi \in \mathrm{Hom}_K(V, W)$ und ist φ^* die zu φ duale Abbildung, so ist*

$$\mathrm{Kern}(\varphi) = (W^*\varphi^*)^{\top} \quad \textit{und} \quad \mathrm{Kern}(\varphi^*) = (\varphi V)^{\perp}.$$

Beweis. Es sei $v \in \mathrm{Kern}(\varphi)$. Dann ist

$$(f\varphi^*)v = f(\varphi v) = 0$$

für alle $f \in W^*$. Daher ist $v \in (W^*\varphi^*)^\top$. Es sei umgekehrt $v \in (W^*\varphi^*)^\top$. Dann ist

$$f(\varphi v) = (f\varphi^*)v = 0$$

für alle $f \in W^*$. Hieraus folgt $\varphi v = 0$ und damit $v \in \mathrm{Kern}(\varphi)$. Also ist $\mathrm{Kern}(\varphi) = (W^*\varphi^*)^\top$.

Es sei $f \in \mathrm{Kern}(\varphi^*)$. Dann ist

$$f(\varphi v) = (f\varphi^*)v = 0$$

für alle $v \in V$, so dass $f \in (\varphi V)^\perp$ gilt. Ist umgekehrt $f \in (\varphi V)^\perp$, so ist

$$(f\varphi^*)v = f(\varphi v) = 0$$

für alle $v \in V$. Daher ist $f\varphi^* = 0$, so dass $f \in \mathrm{Kern}(\varphi^*)$ gilt. Demnach ist $\mathrm{Kern}(\varphi^*) = (\varphi V)^\perp$. Damit ist alles bewiesen.

5.24. Satz. *Es seien V und W Rechtsvektorräume über dem Körper K. Ist $\varphi \in \mathrm{Hom}_K(V,W)$ und ist φ^* die zu φ duale Abbildung, so gilt:*
a) *Genau dann ist φ surjektiv, wenn φ^* injektiv ist.*
b) *Genau dann ist φ injektiv, wenn φ^* surjektiv ist.*
c) *Genau dann ist φ bijektiv, wenn φ^* bijektiv ist.*

Beweis. a) Nach 5.23 ist $\mathrm{Kern}(\varphi^*) = (\varphi V)^\perp$. Ist nun φ^* injektiv, so ist $(\varphi V)^{\perp\top} = \{0\}^\top = W$. Mit 5.18 c) folgt hieraus $\varphi V = W$, so dass φ surjektiv ist. Ist umgekehrt φ surjektiv, so ist $\mathrm{Kern}(\varphi^*) = W^\perp = \{0\}$, also φ^* injektiv.

b) Nach 5.23 ist $\mathrm{Kern}(\varphi) = (W^*\varphi^*)^\top$. Ist φ^* surjektiv, so ist also $\mathrm{Kern}(\varphi) = (V^*)^\top = \{0\}$, so dass φ injektiv ist.

Es sei φ schließlich injektiv. Ferner sei B eine Basis von V. Weil φ injektiv ist, ist $\{\varphi b \mid b \in B\}$ eine Menge von linear unabhängigen Vektoren von W. Es gibt somit einen Teilraum U von W mit

$$W = U \oplus \bigoplus_{b \in B} (\varphi b)K.$$

Ist $g \in V^*$, so definieren wir $f \in W^*$ durch $f(\varphi b) := gb$ für alle $b \in B$ und $fu := 0$ für alle $u \in U$. Es folgt, dass $f\varphi^* = g$ ist. Somit ist φ^* surjektiv.

c) folgt aus a) und b).

5.25. Satz. *Es seien V und W Rechtsvektorräume über K. Ferner sei $\varphi \in \mathrm{Hom}_K(V,W)$ und φ^* sei die zu φ duale Abbildung. Genau dann ist φV endlich erzeugt, wenn $W^*\varphi^*$ endlich erzeugt ist. Ist einer dieser beiden Räume endlich erzeugt, so ist $\mathrm{Rg}(\varphi) = \mathrm{Rg}(\varphi^*)$. Ist V oder W endlich erzeugt, so sind φV und $W^*\varphi^*$ endlich erzeugt.*

Beweis. W und W^* sind gekoppelte Räume und φV ist ein Teilraum von W. Ist nun φV endlich erzeugt, so sind nach 5.16 b) die Räume $(\varphi V)^*$ und

$W^*/(\varphi V)^\perp$ isomorph. Nach 5.14 sind daher die Ränge von φV und $W^*/(\varphi V)^\perp$ gleich. Nach 5.21 ist $(\varphi V)^\perp$ der Kern von φ^*, so dass $W^*\varphi^*$ endlich erzeugt ist und die Ränge von φ und φ^* gleich sind.

Es sei $W^*\varphi^*$ endlich erzeugt. Nach 5.18 d) ist dann

$$W^*\varphi^* = (W^*\varphi^*)^{\top\perp}.$$

Nach 5.16 a) ist daher $W^*\varphi^*$ zu $(v/(W^*\varphi^*)^\top)^*$ isomorph. Nach 5.21 ist daher $(V/\mathrm{Kern}(\varphi))^*$ zu $W^*\varphi^*$ isomorph. Mittels 5.14 folgt, dass φV endlich erzeugt ist. Dann ist aber, wie wir gesehen haben, $\mathrm{Rg}(\varphi) = \mathrm{Rg}(\varphi^*)$.

Ist V oder W endlich erzeugt, so ist in beiden Fällen auch φV endlich erzeugt.

Die Situation von 5.25 verallgemeinernd formulieren wir

5.26. Satz. *Es sei K ein Körper und W und V seien gekoppelte Vektorräume über K. Es sei ferner R ein Ring, W sei ein Rechtsmodul und V ein Linksmodul über R. Wir setzen zudem voraus, dass die folgenden Rechenregeln gelten:*
a) *Es ist $(wr)v = w(rv)$ für alle $r \in R$, alle $w \in W$ und alle $v \in V$.*
b) *Es ist $(kw)r = k(wr)$ für alle $k \in K$, alle $w \in W$ und alle $r \in R$.*
c) *Es ist $(rv)k = r(vk)$ für alle $r \in R$, alle $v \in V$ und alle $k \in K$.*
Ist $r \in R$, so ist rV genau dann endlich erzeugt, wenn Wr endlich erzeugt ist. Ist dies der Fall, so gilt $\mathrm{Rg}_K(rV) = \mathrm{Rg}^K(Wr)$.

Beweis. Setze $Y := (rV)^\perp$. Ist dann $y \in Y$ und $v \in V$, so folgt $(yr)v = y(rv) = 0$. Wegen $V^\perp = \{0\}$ ist daher $yr = 0$. Ist andererseits $w \in W$ und $wr = 0$, so folgt $0 = (wr)v = w(rv)$ für alle $v \in V$, so dass $w \in Y$ gilt. Es folgt, dass Wr zu W/Y isomorph ist. Nach Früherem ist Wr daher endlich erzeugt und es gilt $\mathrm{Rg}^K(Wr) = \mathrm{Rg}_K(rV)$. Aus Symmetriegründen ist damit alles gezeigt.

Dieser Satz wird später noch eine Rolle spielen.

6. Homogene, vollständig reduzible Ringe

In diesem Abschnitt greifen wir, wie versprochen, die Frage nach der Struktur der homogenen, vollständig reduziblen Ringe wieder auf. Kennen wir diese, so kennen wir auf Grund von Satz 4.6 alle vollständig reduziblen Ringe, da die ringtheoretische direkte Summe von homogenen, vollständig reduziblen Ringen ein vollständig reduzibler Ring ist.

Wir definieren das *Jacobson-Radikal* $J(R)$ eines Ringes R als den Schnitt über alle regulären, maximalen Rechtsideale von R. Ist M ein irreduzibler R-Rechtsmodul und ist $0 \neq x \in M$, so ist $O(x)$ nach 4.2 ein reguläres, maximales Rechtsideal. Daher ist $J(R) \subseteq O(x)$, so dass $xj = 0$ ist für alle $j \in J(R)$. Somit gilt $MJ(R) = \{0\}$ für alle irreduziblen R-Rechtsmoduln M. Ist I ein reguläres, maximales Rechtsideal von R, so ist R/I nach 4.2 ein irreduzibler R-Modul. Nach der gerade gemachten Bemerkung ist daher $RJ(R) \subseteq I$. Da dies für alle regulären, maximalen Ideale gilt, folgt $RJ(R) \subseteq J(R)$, so dass $J(R)$ ein zweiseitiges Ideal von R ist.

6.1. Satz. *Ist R ein vollständig reduzibler Ring, so ist $J(R) \neq R$ und $J(R)^2 = \{0\}$.*

Beweis. Es sei I ein minimales Rechtsideal, welches in $J(R)$ enthalten ist. Dann ist I ein irreduzibler R-Rechtsmodul. Daher ist $IR \neq \{0\} = IJ(R)$. Hieraus folgt $R \neq J(R)$. Weil $J(R)$ Summe von minimalen Rechtsidealen von R ist, folgt, dass auch $J(R)^2 = \{0\}$ gilt.

6.2. Satz. *Ist R ein vollständig reduzibler Ring und ist I ein minimales Rechtsideal von R, so gilt genau dann $I \subseteq J(R)$, wenn $I^2 = \{0\}$ ist.*

Beweis. Ist $I \subseteq J(R)$, so ist $I^2 \subseteq J(R)^2 = \{0\}$.

Es sei $I \not\subseteq J(R)$. Es gibt dann ein reguläres, maximales Rechtsideal M von R, welches I nicht enthält. Es folgt $R = I \oplus M$ als R-Rechtsmodul. Weil M regulär ist, gibt es ein $a \in R$ mit $x - ax \in M$ für alle $x \in R$. Es ist $a = i + m$ mit $i \in I$ und $m \in M$. Es folgt, dass auch $x - ix \in M$ gilt für alle $x \in R$. Insbesondere ist also

$$i - i^2 \in I \cap M = \{0\}.$$

Also ist $i^2 = i$. Nun ist aber $i \neq 0$, da andernfalls $R = M$ wäre. Somit ist $I^2 \neq \{0\}$.

Im Verlaufe des Beweises des letzten Satzes haben wir gezeigt, dass das minimale Ideal I ein von Null verschiedenes Idempotent enthält, wenn I nicht im Jacobson-Radikal des Ringes liegt. Allgemeiner gilt:

6.3. Satz *Es sei R ein Ring und I sei ein minimales Rechtsideal von R. Ist $I^2 \neq \{0\}$, so gibt es ein von 0 verschiedenes Idempotent $i \in I$. Insbesondere ist $I = iR$.*

Beweis. Wegen $I^2 \neq \{0\}$ gibt es ein $x \in I$ mit $xI \neq \{0\}$. Weil xI ein in I enthaltenes Rechtsideal ist, folgt wegen der Minimalität von I daher, dass $xI = I$ ist. Es gibt also ein $i \in I$ mit $xi = x$. Es folgt $x(i^2 - i) = 0$. Setze $I' := \{y \mid y \in I, xy = 0\}$. Dann ist I' ein Rechtsideal, welches in I enthalten ist. Nun ist $x \neq 0$ und daher $i \in I'$. Folglich ist $I' = \{0\}$. Wegen $i^2 - i \in I'$ ist also $i^2 = i$.

Schließlich ist $i = i^2 \in iR \subseteq I$ und somit $iR = I$ auf Grund der Minimalität von I.

6.4. Satz. *Es sei R ein homogener, vollständig reduzibler Ring. Ferner sei S die Summe über alle minimalen Ideale I von R, für die $I^2 \neq \{0\}$ gilt. Dann ist S ein einfacher, vollständig reduzibler Ring und es gilt im modultheoretischen Sinne*

$$R = J(R) \oplus S.$$

Sind j, $j' \in J(R)$ und s, $s' \in S$, so ist

$$(j + s)(j' + s') = js' + ss'.$$

Beweis. Weil R die Summe seiner minimalen Rechtsideale ist, folgt zunächst, dass $RJ(R) = \{0\}$ ist. Ferner folgt mit 6.2, dass R im modultheoretischen Sinne

die direkte Summe von $J(R)$ und S ist. Weil S ein Rechtsideal ist, ist natürlich $SS \subseteq S$, so dass S ein Ring ist.

Es sei I ein minimales Rechtsideal von R, welches in S enthalten ist. Ist $0 \neq x \in I$, so gilt

$$I = xR \subseteq xJ(R) + xS = xS \subseteq I.$$

Daher ist I auch ein minimales Rechtsideal von S. Da S Summe minimaler Rechtsideale von R ist, folgt hieraus schon, dass S vollständig reduzibel ist.

Es sei nun N ein von $\{0\}$ verschiedenes, zweiseitiges Ideal von S. Wegen

$$NR \subseteq NJ(R) + NS = NS \subseteq N$$

ist N ein Rechtsideal von R. Es gibt also ein minimales Rechtsideal I von R, welches in N enthalten ist. Nach der Definition von S gilt $I^2 \neq \{0\}$, so dass I nach 6.3 ein von Null verschiedenes Idempotent n enthält. Es sei I' ein weiteres minimales Rechtsideal von R, welches in S enthalten ist. Weil R homogen ist, gibt es einen R-Isomorphismus σ von I auf I'. Setze $i := \sigma(n)$. Dann ist

$$0 \neq i = \sigma(n) = \sigma(n^2) = in \in I' \cap N.$$

(Dieses Argument haben wir schon einmal gefeiert.) Weil I', wie wir gesehen haben, auch ein minimales Rechtsideal von S ist, folgt $I' \subseteq N$. Benutzt man nun noch einmal, dass S die Summe über alle minimalen Rechtsideale von R ist, deren Quadrat nicht Null ist, so folgt, dass $N = S$ ist, womit die Einfachheit von S nachgewiesen ist.

Ist $r \in R$ und $j \in J(R)$, so ist $rj = 0$, wie zuvor schon bemerkt. Hieraus folgt schließlich auch noch die Gültigkeit der letzten Behauptung des Satzes.

Ist S ein einfacher, vollständig reduzibler Ring und ist M ein S-Rechtsmodul mit $MS = M$, so zeigt Satz 6.4, wie man aus S und M einen homogenen, vollständig reduziblen Ring R machen kann, so dass M gerade das Jacobson-Radikal von R wird. Man kennt also alle homogenen, vollständig reduziblen Ringe, wenn man alle einfachen, vollständig reduziblen Ringe kennt. Um diese besser in den Griff zu kriegen, beweisen wir zunächst das schursche Lemma, welches ein überaus nützliches Werkzeug ist.

6.5. Schursches Lemma. *Es sei R ein Ring und M sei ein irreduzibler R-Modul. Dann ist* $\mathrm{End}_R(M)$ *ein Körper.*

Beweis. Es sei $0 \neq \sigma \in \mathrm{End}_R(M)$. Dann ist $\sigma(M)$ ein von $\{0\}$ verschiedener Teilmodul von M. Somit gilt wegen der Irreduzibilität von M die Gleichung $\sigma(M) = M$, so dass σ surjektiv ist. Ferner gilt $\mathrm{Kern}(\sigma) \neq M$ und daher $\mathrm{Kern}(\sigma) = \{0\}$, so dass σ auch injektiv ist. Folglich ist σ ein Automorphismus von M, so dass σ eine Einheit von $\mathrm{End}_R(M)$ ist. Damit ist alles bewiesen.

Es sei R ein Ring und M sei ein R-Rechtsmodul. Man nennt M *treuen* R-Rechtsmodul, falls aus $r \in R$ und $Mr = \{0\}$ folgt, dass $r = 0$ ist. Der Ring R heißt *primitiv*, falls er einen treuen, irreduziblen Modul besitzt.

6.6. Satz. *Es sei R ein primitiver Ring und M sei ein treuer, irreduzibler R-Rechtsmodul. Setze $K :=$* $\mathrm{End}_R(M)$. *Dann ist K ein Körper und M ist*

ein Linksvektorraum über K. Es bezeichne $E^K(M)$ die Menge der Teilräume endlichen Ranges des K-Vektorraumes M. Für $X \in E^K(M)$ sei $O(X) := \{r \mid r \in R,\ Xr = \{0\}\}$. Dann ist O ein Monomorphismus von $E^K(V)$ in $L_R(R)$ mit der Eigenschaft, dass für X, $Y \in E^K(V)$ genau dann $X \leq Y$ gilt, wenn $O(Y) \subseteq O(X)$ ist.

Beweis. Dass K ein Körper ist, besagt gerade das schursche Lemma.

Aus der Definition von O folgt, dass $X \leq Y$ impliziert, dass $O(Y) \subseteq O(X)$ ist. Wir zeigen, dass aus $X < Y$ folgt, dass $O(Y) \subset O(X)$ ist. Dazu machen wir Induktion nach dem Rang von X. Es sei $y \in Y - X$. Ist der Rang von X gleich 0, so ist $X = \{0\}$. Weil M irreduzibel ist, ist $yR = M$, so dass es ein $s \in R$ gibt mit $ys \neq 0$. Also ist $O(Y) \subset R = O(X)$.

Der Rang von X sei nun größer als 0 und w sei ein von 0 verschiedener Vektor in X. Es gibt dann einen Teilraum V von X mit $X = V \oplus Kw$. Wir nehmen nun an, dass $O(X) \subseteq O(y)$ gelte, wobei y immer noch das oben gewählte Element ist. Nach Induktionsannahme ist $O(V) \not\subseteq O(w)$, da andernfalls $O(V) = O(X)$ wäre. Daher ist $wO(V)$ ein von $\{0\}$ verschiedener Teilmodul von M. Folglich gilt $wO(V) = M$. Es seien a, $b \in O(V)$ und es gelte $wa = wb$. Dann ist

$$a - b \in O(w) \cap O(V) = O(X) \subseteq O(y),$$

so dass $ya = yb$ ist. Folglich wird durch $\kappa(wa) := ya$ ein Endomorphismus κ des R-Rechtsmoduls $wO(V) = M$ definiert, dh., es gilt $\kappa \in K$. Es folgt $(\kappa w - y)a = 0$ für alle $a \in O(V)$. Nach Induktionsannahme ist daher $\kappa w - y \in V$ und daher $y \in V + Kw = X$. Dieser Widerspruch zeigt, dass $O(X) \not\subseteq O(y)$ ist. Folglich ist $O(Y) \subset O(X)$. Es sei schließlich $O(Y) \subseteq O(X)$. Dann ist

$$O(X + Y) = O(X) \cap O(Y) = O(Y).$$

Wegen $Y \leq X + Y$ ist daher nach dem bereits Bewiesenen $Y = X + Y$, so dass $X \leq Y$ gilt. Damit ist alles bewiesen.

6.7. Dichtesatz. *Es sei R ein primitiver Ring und M sei ein irreduzibler Rechtsmodul über R. Setze $K := \mathrm{End}_R(M)$. Dann ist K ein Körper und M ist ein Linksvektorraum über K. Ist dann n eine natürliche Zahl, sind $b_1, \ldots, b_n$ linear unabhängige Elemente des K-Vektorraumes M und sind $v_1, \ldots, v_n$ irgendwelche Elemente von M, so gibt es ein $r \in R$ mit $b_i r = v_i$ für $i := 1, \ldots, n$.*

Beweis. Nach 6.6 gibt es Elemente $s_i \in R$ mit $b_j s_i = 0$ für $j \neq i$ und $b_i s_i \neq 0$. Es folgt weiter, dass $(b_i s_i)R = M$ ist. Es gibt also ein $t_i \in R$ mit $b_i s_i t_i = v_i$. Setzt man nun $r := \sum_{j:=1}^n s_j t_j$, so ist

$$b_i r = \sum_{j:=1}^n b_i s_j t_j = b_i s_i t_i = v_i.$$

Damit ist der Dichtesatz bewiesen.

Man nennt einen Ring R *artinsch*, wenn der Verband der Rechtsideale von R artinsch ist.

6.8. Satz. *Es sei R ein primitiver Ring. Genau dann gibt es einen Rechtsvektorraum V endlichen Ranges über einem Körper K, so dass R zu $\mathrm{End}_K(V)$ isomorph ist, wenn R artinsch ist. Insbesondere enthält jeder solche Ring eine Eins.*

Beweis. Es sei V ein Rechtsvektorraum endlichen Ranges über dem Körper K. Dann ist $J_K(V) = \mathrm{End}_K(V)$, so dass $\mathrm{End}_K(V)$ nach 4.15 artinsch ist. Somit ist R artinsch, wenn R zu $\mathrm{End}_K(V)$ isomorph ist.

Es sei R artinsch. Ferner sei M ein treuer, irreduzibler R-Rechtsmodul. Dann ist M ein Linksvektorraum über dem Körper $K := \mathrm{End}_R(M)$. Setze

$$\Psi := \bigl\{O(X) \mid X \in E^K(M)\bigr\}.$$

Weil R artinsch ist, enthält Ψ ein minimales $O(Y)$. Nach 6.6 ist Y dann ein maximales Element von $E^K(M)$. Es folgt, dass $Y = M$ ist. Ist n der Rang von M und ist $b_1, \ldots, b_n$ eine Basis von M, sind ferner $v_1, \ldots, v_n$ irgendwelche Elemente von M, so gibt es nach dem Dichtesatz ein $r \in R$ mit $b_i r = v_i$ für alle i. Hieraus folgt, da R auf M ja treu operiert, dass R zu $\mathrm{End}^K(M)$ isomorph ist. Ist V der Dualraum des K-Linksvektorraumes M, so folgt mit 5.20, dass R auch zu $\mathrm{End}_K(V)$ isomorph ist.

6.9. Satz. *Es sei R ein Ring. Dann sind die folgenden Bedingungen äquivalent:*
a) *R ist als Ring die direkte Summe von endlich vielen Endomorphismenringen von Rechtsvektorräumen endlichen Ranges.*
b) *R ist vollständig reduzibel und hat eine Eins.*
c) *R ist artinsch und für jedes minimale Rechtsideal I von R gilt $I^2 \neq \{0\}$.*

Beweis. Endomorphismenringe von Rechtsvektorräumen endlichen Ranges haben eine Eins und sind nach 4.13 vollständig reduzibel sind; daher ist b) eine Folge von a).

Es gelte b). Nach 4.6 ist $R = \bigoplus_{\Phi \in I_R(R)/\equiv} H_\Phi$. Weil R eine Eins hat, gibt es endlich viele homogene Komponenten $H_1, \ldots, H_t$ von R mit $1 \in \sum_{k:=1}^t H_k$. Es folgt $R \subseteq \sum_{k:=1}^t H_k$, so dass R nur endlich viele homogene Komponenten hat. Ist H eine von ihnen, so ist H die Summe von minimalen Rechtsidealen. Mit dem gleichen Argument erhält man, dass H Summe von endlich vielen minimalen Rechtsidealen ist. Hieraus folgt, dass der Rechtsidealverband von H eine projektive Geometrie endlichen Ranges ist. Da R die direkte Summe von endlich vielen homogenen Komponenten ist, ist R daher artinsch. Es sei schließlich I ein minimales Ideal von R. Weil R vollständig reduzibel ist, gibt es ein Rechtsideal J mit $R = I \oplus J$. Es gibt daher ein $i \in I$ und ein $j \in J$ mit $1 = i + j$. Es folgt

$$i = 1i = i^2 + ji$$

und weiter

$$ji = i - i^2 \in I \cap J = \{0\}.$$

Also ist $i^2 = i$. Wäre nun $i = 0$, so wäre $1 \in J$ und daher $R \subseteq J$. Also ist $i \neq 0$, so dass auch $I^2 \neq \{0\}$ ist. Damit ist c) aus b) hergeleitet.

Es gelte c). Weil R artinsch ist, gibt es zu jedem von $\{0\}$ verschiedenen Rechtsideal J von R ein minimales Rechtsideal I mit $I \subseteq J$. Es gibt also eine Auswahlfunktion μ, so dass $\mu(J)$ für alle solchen J ein minimales, in J enthaltenes Rechtsideal ist. Setzt man noch $\mu(\{0\}) := \{0\}$, so ist μ auf der Menge aller Rechtsideale von R definiert.

Auf Grund unserer Annahme über die minimalen Rechtsideale von R gibt es nach 6.3 eine Auswahlfunktion e, so dass e_I für alle minimalen Rechtsideale I ein Idempotent ist, welches in I liegt und von 0 verschieden ist. Ist I das Nullideal, so setzen wir noch $e_I = 0$. Es sei nun I ein minimales Rechtsideal von R. Dann ist $e_I \notin O(e_I)$. Andererseits ist $O(e_I)$ nach 4.2 ein reguläres, maximales Rechtsideal. Daher gilt

$$R = I + O(e_I).$$

Aus dem dedekindschen Rekursionssatz folgt die Existenz einer Abbildung g der Menge der nicht negativen Zahlen in die Menge der Rechtsideale von R mit $g(0) = R$ und

$$g(n+1) = g(n) \cap O(e_{\mu(g(n))}).$$

Es folgt

$$g(n) = g(n) \cap \big(\mu(g(n)) + O(e_{\mu(g(n))})\big) = \mu\big(g(n)\big) + g(n+1).$$

Mittels Induktion folgt die Gültigkeit von

$$R = \sum_{i:=0}^{n} \mu\big(g(i)\big) + g(n+1)$$

für alle n. Nun ist aber $g(n+1) \subseteq g(n)$ für alle n. Weil R artinsch ist, gibt es also ein N mit $g(N) = g(N+1)$. Hieraus folgt weiter

$$\mu\big(g(N)\big) \subseteq g(N) \cap O(e_{\mu(g(N))}).$$

Dies hat

$$R = \mu\big(g(N)\big) + O(e_{\mu(g(N))}) = O(e_{\mu(g(N))})$$

zur Folge, was wiederum $g(N) = \{0\}$ nach sich zieht. Also ist R Summe von minimalen Rechtsidealen und folglich, da deren Quadrat ja niemals das Nullideal ist, vollständig reduzibel.

Nach 4.6 ist R direkte Summe seiner homogenen Komponenten, von denen es nur endlich viele gibt, da R artinsch ist. Mittels 6.2 und 6.4 folgt weiter, dass die homogenen Komponenten von R allesamt einfache Ringe sind. Einfache, vollständig reduzible Ringe sind aber stets primitiv. Mittels 6.8 folgt dann, dass die homogenen Komponenten von R zu Endomorphismenringen von Rechtsvektorräumen isomorph sind. Damit ist a) aus c) hergeleitet und der Satz bewiesen.

Die Bedingung c) wird in der Literatur meist so formuliert, dass man sagt, R sei ein halbeinfacher, artinscher Ring, wobei *halbeinfach* bedeutet, dass $J(R) =$

$\{0\}$ ist. Benutzt man diese Formulierung, so muss man zeigen, dass das Jacobson-Radikal eines Ringes R alle nilpotenten Rechtsideale von R enthält. Ferner muss man zeigen, dass das Jacobson-Radikal eines artinschen Ringes nilpotent ist.

Der soeben bewiesene Satz ist grundlegend für die Darstellungstheorie endlicher Gruppen, wie wir gleich belegen werden. Zuvor jedoch müssen wir noch den Begriff der *Gruppenalgebra* einer endlichen Gruppe einführen. Dazu sei K ein kommutativer Körper und G sei eine endliche Gruppe. Wir interpretieren G als Basis eines Vektorraumes $K[G]$ über K, von dem wir auf Grund der Kommutativität von K annehmen dürfen, dass er zweiseitig ist. Sind dann $x := \sum_{g \in G} k_g g$ und $y := \sum_{h \in G} l_h h$ zwei Elemente von $K[G]$, so definieren wir ihr Produkt xy durch

$$xy := \sum_{g \in G} \sum_{\substack{a,b \in G \\ ab=g}} k_a l_b g.$$

Auf diese Weise wird $K[G]$ zu einer K-Algebra, der Gruppenalgebra von G über K. Es gilt nun der

6.10. Satz von Maschke. *Ist K ein kommutativer Körper, ist G eine endliche Gruppe und ist $K[G]$ ihre Gruppenalgebra über K, so ist $K[G]$ ein artinscher Ring mit Eins. Genau dann ist $K[G]$ vollständig reduzibel, wenn die Charakteristik von K kein Teiler von $|G|$ ist.*

Beweis. Die Eins von G ist auch die Eins von $K[G]$. Dass $K[G]$ artinsch ist, liegt daran, dass $K[G]$ ein Vektorraum endlichen Ranges über K ist. Damit ist der banale Teil des Satzes bewiesen.

Die Charakteristik von K sei ein Teiler von $|G|$. Setze $a := \sum_{g \in G} g$. Weil G eine Basis von $K[G]$ ist, ist $a \neq 0$. Ist $x \in G$, so ist $ax = a = xa$, so dass a im Zentrum von $K[G]$ liegt. Dies beinhaltet, dass $aK[G]$ ein vom Nullideal verschiedenes, zweiseitiges Ideal von $K[G]$ ist. Nun ist

$$a^2 = a \sum_{g \in G} g = |G|a = 0.$$

Daher ist $(aK[G])^2 = \{0\}$. Weil R artinsch ist, enthält $aK[G]$ ein minimales Rechtsideal I. Für dieses gilt dann $I^2 = \{0\}$, so dass $K[G]$ nach 6.9 nicht vollständig reduzibel ist.

Es sei $K[G]$ nicht vollständig reduzibel. Dann enthält $K[G]$ nach 6.9 ein minimales Rechtsideal I mit $I^2 = \{0\}$. Es sei $0 \neq i \in I$. Dann ist $i = \sum_{g \in G} k_g g$, wobei es wenigstens ein $h \in G$ gibt mit $k_h \neq 0$. Dann ist auch ih^{-1} ein von 0 verschiedenes Element von I, so dass wir annehmen dürfen, dass in der Entwicklung für i das Element k_1 von Null verschieden ist.

Ist $a \in K[X]$, so ist die Abbildung α_a, die durch $\alpha_a(x) := xa$ für alle $x \in K[G]$ definiert wird, eine K-lineare Abbildung von $K[G]$ in sich. Ist insbesondere $a \in G$, so ist $\mathrm{Spur}(\alpha_a) = 0$, wenn $a \neq 1$ gilt, und $\mathrm{Spur}(\alpha_a) = |G|$, wenn $a = 1$ ist. Hieraus folgt

$$\mathrm{Spur}(\alpha_i) = \sum_{g \in G} k_g \mathrm{Spur}(\alpha_g) = k_1 |G|.$$

Nun ist aber $i^2 = 0$, so dass alle Eigenwerte von α_i gleich 0 sind. Dann ist aber auch die Spur von α gleich 0, da sie die Summe der Eigenwerte ist. Also ist $k_1|G| = 0$. Weil k_1 aber nicht 0 ist, ist $|G|$ in K gleich 0. Folglich ist die Charakteristik von K ein Teiler von $|G|$. Damit ist der Satz von Maschke bewiesen.

Zusammen mit Satz 6.9 besagt der Satz von Maschke, dass der Gruppenring einer endlichen Gruppe, falls die Charakteristik des zu Grunde liegenden kommutativen Körpers die Gruppenordnung nicht teilt, die direkte Summe von endlich vielen Endomorphismenringen von Vektorräumen endlichen Ranges ist. Es ist zu beachten, dass die Körper, über denen diese Vektorräume definiert sind, zwar alle K enthalten, aber durchaus nicht immer gleich K sind. Einzelheiten findet der Leser in den Büchern zur Darstellungstheorie endlicher Gruppen.

Wir wenden uns nun wieder der Untersuchung beliebiger einfacher, vollständig reduzibler Ringe zu. Dabei folgen wir bislang unveröffentlichten Notizen von Herrn U. Dempwolff.

6.11. Satz. *Es sei R ein einfacher, vollständig reduzibler Ring und M sei ein treuer, irreduzibler Rechtsmodul über R. Setze*

$$K := \mathrm{End}_R(M).$$

Dann ist K ein Körper und M ist ein Linksvektorraum über K. Weil R auf M treu operiert, dürfen wir $R \subseteq \mathrm{End}^K(M)$ annehmen. Wir setzen

$$\Xi := \bigl\{U \mid U \in L^K(M) \text{ und es gibt ein } r \in R \text{ mit } U = \mathrm{Kern}(r)\bigr\}.$$

Dann gilt:
a) *Ist $U \in \Xi$, so ist $\mathrm{KoRg}^M(U)$ endlich, dh. es ist $R \subseteq J^K(M)$.*
b) *Ist $U \in \Xi$, ist $V \in L^K(M)$ und gilt $U \leq V$, so ist $V \in \Xi$.*
c) *Sind U, $V \in \Xi$, so ist auch $U \cap V \in \Xi$.*
d) *Es ist $\bigcap_{U\in\Xi} U = \{0\}$.*

Ferner gilt: $R = \bigl\{r \mid r \in \mathrm{End}^K(M), \mathrm{Kern}(r) \in \Xi\bigr\}$.

Beweis. Wir beweisen zunächst

1) Genau dann ist I ein minimales Rechtsideal von R, wenn es eine Hyperebene $H \in \Xi$ gibt mit $I = O(H)$. Ist I ein minimales Rechtsideal, so gibt es ein Idempotent $\pi \in I$ mit $I = \pi R$.

Es sei I ein minimales Rechtsideal von R. Weil R einfach ist, gibt es dann nach 6.4 und 6.3 ein Idempotent $\pi \in I$ mit $I = \pi R$. Setze $H := \{m - m\pi \mid m \in M\}$. Dann ist $H \in L^K(M)$. Überdies gilt $H \leq \mathrm{Kern}(\pi)$. Ist andererseits $m \in \mathrm{Kern}(\pi)$, so ist $m = m - m\pi \in H$, so dass $H = \mathrm{Kern}(i)$ ist. Es seien nun u und v zwei Elemente von M, so dass $u\pi$ und $v\pi$ linear unabhängig sind. Auf Grund des Dichtesatzes, der ja für R gilt, gibt es dann ein $r \in R$, so dass $u\pi r \neq 0$ und $v\pi r = 0$ ist. Es folgt $0 \neq \pi r \in I$ und damit $\pi r R = I$. Es gibt also ein $s \in R$ mit $\pi rs = \pi$. Es folgt der Widerspruch $v\pi = v\pi rs = 0$. Damit ist gezeigt, dass H eine Hyperebene von M ist. Es gilt ferner, dass $I = \pi R \subseteq O(H)$ ist. Es sei $s \in O(H)$ und $m \in M$. Dann ist $m = m\pi + m - m\pi$. Es folgt $ms = m\pi s$, so dass $s = \pi s \in I$ gilt. Somit ist $I = O(H)$.

Es sei H eine Hyperebene, die zu Ξ gehört. Es gibt dann ein $\lambda \in R$ mit $\mathrm{Kern}(\lambda) = H$. Es folgt $\lambda R \subseteq O(H)$. Weil $\lambda \neq 0$ ist, gibt es ein in λR enthaltenes minimales Rechtsideal I von R. Wie wir bereits gesehen haben, enthält I ein Idempotent π mit $\pi R = I = O(\mathrm{Kern}(\pi))$. Weil $\mathrm{Kern}(\pi)$ eine Hyperebene ist, die H enthält, ist $H = \mathrm{Kern}(\pi)$. Somit ist $O(H) = I \subseteq \lambda R \subseteq O(H)$, so dass $O(H)$ in der Tat ein minimales Rechtsideal ist.

2) Es seien $H_1, \ldots, H_t$ Hyperebenen, die zu Ξ gehören. Setze

$$V_i := \bigcap_{k:=1,\ldots,t,\ k \neq i} H_k$$

für $i := 1, \ldots, t$. Es gelte ferner

$$V_i \not\leq H_i$$

für $i := 1, \ldots, t$. Es gibt dann ein Idempotent $\pi \in R$ mit $\bigcap_{i:=1}^t H_i = \mathrm{Kern}(\pi)$. Insbesondere ist $O(\bigcap_{i:=1}^t H_i) = \pi R$.

Ist $t = 1$, so ist dies richtig nach 1). Es sei also $t \geq 2$. Wir setzen

$$U := \bigcap_{i:=1}^t H_i.$$

Es gibt dann $a_i \in V_i$ mit $V_i = Ka_i \oplus U$. Auf Grund der Annahme über die Hyperebenen ist

$$M = U + \sum_{i:=1}^t Ka_i.$$

Zu jedem i gibt es nach 1) ein Idempotent π_i mit $\mathrm{Kern}(\pi_i) = H_i$. Weil $V_i \not\leq H_i$ gilt, folgt $a_i\pi_i \neq 0$. Daher gelten die Gleichungen

$$\begin{aligned} a_1 O(H_1) &= M, \\ a_2 O(H_2) &= M, \\ &\vdots \\ a_t O(H_t) &= M. \end{aligned}$$

Es gibt also $\lambda_i \in O(H_i)$ mit $a_i\lambda_i = a_i$. Ist $i \neq j$, so ist $a_j \in H_i$, so dass $a_j\lambda_i = 0$ ist. Setze $\pi := \sum_{i:=1}^t \lambda_i$. Ist nun $m \in M$, so gibt es $k_i \in K$ und ein $u \in U$ mit

$$m = u + \sum_{i:=1}^t k_i a_i.$$

Dann folgt $m\lambda_i = k_i a_i$ und weiter

$$m\pi = \sum_{i:=1}^t k_i a_i.$$

Weil die a_i linear unabhängig sind, folgt, dass der Kern von π gleich U ist. Ferner folgt $m\pi^2 = m\pi$ für alle $m \in M$, so dass π in der Tat ein Idempotent ist.

Um auch die letzte Aussage zu beweisen, bemerken wir zunächst, dass $\pi R \subseteq O(\bigcap_{i:=1}^t H_i)$ gilt. Es sei $r \in O(\bigcap_{i:=1}^t H_i)$. Ist dann wieder $m = u + \sum_{i:=1}^t k_i a_i$, so folgt

$$mr = \sum_{i:=1}^t k_i a_i r = m\pi r.$$

Also ist $r = \pi r \in \pi R$. Damit ist 2) bewiesen.

Als Nächstes beweisen wir:

3) Es seien $H_1, \ldots, H_t$ Hyperebenen, die zu Ξ gehören. Setze

$$V_i := \bigcap_{k:=1,\ldots,t,\ k\neq i} H_k$$

für $i := 1, \ldots, t$. Es gelte ferner

$$V_i \not\leq H_i$$

für $i := 1, \ldots, t$. Ist dann H eine Hyperebene von M mit $\bigcap_{i:=1}^t H_i \leq H$, so ist $H \in \Xi$.

Dies ist richtig, falls H gleich einem der H_i ist. Dies ist sicher dann der Fall, wenn $t = 1$ ist. Wir dürfen daher annehmen, dass H von allen H_i verschieden ist und dass der Satz für $t-1$ gilt. Wendet man 2.6 auf $L^K(M/\bigcap_{i:=1}^t H_i)^d$ an, so folgt die Existenz einer Hyperebene H' mit $H_1 \cap H' \leq H$ und $\bigcap_{i:=2}^t H_i \leq H'$. Wir dürfen daher annehmen, dass $t = 2$ und — nach Induktionsannahme — dass $H' = H_2$ ist. Weil H von H_1 und H_2 verschieden ist, gibt es ein von Null verschiedenes $p \in H$ mit $H = Kp \oplus (H_1 \cap H_2)$. Es folgt $pO(H_1) = M$ und $pO(H_2) = M$. Es gibt also ein $r_i \in O(H_i)$ für $i := 1, 2$ mit $pr_1 = p = -pr_2$. Setze $f := r_1 + r_2$. Dann ist $H \leq \mathrm{Kern}(f)$, wie man unmittelbar sieht. Wäre $f = 0$, so folgte $r_1 = -r_2$. Weil weder r_1 noch r_2 Null sind, folgte mit 1) weiter $O(H_1) = r_1 R = r_2 R = O(H_2)$, da die Ideale $O(H_i)$ ja minimal sind. Hieraus folgte aber der Widerspruch $H_1 = H_2$. Also ist $f \neq 0$ und daher $\mathrm{Kern}(f) = H$.

a) Es sei $r \in R$. Es gibt dann endlich viele minimale Rechtsideale $I_1, \ldots, I_t$ mit $r \in \sum_{k:=1}^t I_k$. Nach 1) gibt es Hyperebenen $H_1, \ldots, H_t$ mit $O(H_k) = I_k$. Ist $m \in \bigcap_{k:=1}^t H_k$, so folgt $mr = 0$, so dass

$$\bigcap_{k:=1}^t H_k \leq \mathrm{Kern}(r)$$

gilt. Folglich hat $\mathrm{Kern}(r)$ endlichen Ko-Rang, so dass a) bewiesen ist.

b) Wir haben gerade gesehen, dass es Hyperebenen $H_1, \ldots, H_t \in \Xi$ gibt mit $\bigcap_{i:=1}^t H_i \leq U$. Da alle Hyperebenen von M, die oberhalb des Schnitts der H_i liegen, nach 3) zu Ξ gehören, und da V Schnitt von endlich vielen dieser Hyperebenen ist, gehört auch V nach 2) zu Ξ.

Der Beweis von c) ist analog dem von b).

d) Es sei schließlich $m \in \bigcap_{U \in \Xi} U$. Dann ist $mR = \{0\}$ und daher $m = 0$, da M ja irreduzibel ist. Damit ist auch d) bewiesen.

Um die letzte Aussage zu beweisen, sei $U \in \Xi$. Da U sich dann als Schnitt von unabhängigen Hyperebenen darstellen lässt, die alle zu Ξ gehören, gibt es eine Projektion π mit $O(U) = \pi R$. Es folgt, dass $M = M\pi \oplus U$ ist. Es sei nun $a_1, \ldots, a_n$ eine Basis von $M\pi$. Ferner sei $s \in \mathrm{End}^K(M)$ und es gelte $U \leq \mathrm{Kern}(s)$. Auf Grund des Dichtesatzes gibt es ein $r \in R$ mit $a_i r = a_i s$ für alle i. Hieraus folgt $a_i \pi r = a_i s$ für alle i. Da U sowohl von πr als auch von s annulliert wird, gilt also $s = \pi r \in R$. Damit ist alles bewiesen.

Eine unmittelbare Folgerung aus der Aussage 2) des Beweises von 6.11 notieren wir als

6.12. Korollar. *Ist R ein einfacher, vollständig reduzibler Ring, so gibt es zu jedem endlich erzeugten Rechtsideal I von R ein Idempotent $\pi \in I$ mit $I = \pi R$.*

Die Teilmenge I des Verbandes L heißt *duales Ideal* von L, wenn aus $A, B \in I$ stets auch $A \cap B \in I$ folgt und mit A auch alle X mit $A \leq X$ zu I gehören. Die in Satz 6.11 definierte Menge Ξ ist also ein duales Ideal von $L^K(M)$.

6.13. Satz. *Es sei K ein Körper und M sei ein von $\{0\}$ verschiedener Linksvektorraum über K. Ferner sei Ξ ein duales Ideal von $L^K(M)$ aus Unterräumen endlichen Ko-Ranges und es gelte $\bigcap_{U \in \Xi} u = 0$. Ist dann*

$$R := \big\{r \mid r \in \mathrm{End}^K(M),\ \mathrm{Kern}(r) \in \Xi\big\},$$

so ist R einfach und vollständig reduzibel. Überdies ist M ein treuer, irreduzibler R-Rechtsmodul.

Beweis. Weil M nicht trivial ist, folgt aus $\bigcap_{U \in \Xi} U = \{0\}$, dass Ξ nicht leer ist. Weiter folgt, dass es zu linear unabhängigen $a_1, \ldots, a_n$ ein $U \in \Xi$ gibt mit $(\sum_{i:=1}^n Ka_i) \cap U = \{0\}$. Um dies einzusehen, setzen wir

$$X := \sum_{i:=1}^n Ka_i.$$

Weil X endlichen Rang hat, gibt es dann ein $U \in \Xi$, so dass $X \cap U$ von minimalen Rang ist. Ist nun $W \in \Xi$, so ist auch $U \cap W \in \Xi$. Hieraus folgt, dass

$$X \cap U \cap W = X \cap U$$

ist. Somit ist $X \cap U \leq W$ für alle $W \in \Xi$. Folglich ist $X \cap U = \{0\}$, wie behauptet. Es gibt nun ein Komplement V von $\sum_{i:=1}^n Ka_i$ in M mit $U \leq V$. Sind $x_1, \ldots, x_n$ beliebige Elemente von M, so definieren wir $r \in \mathrm{End}^K(M)$ durch $a_i r := x_i$ und $vr := 0$ für alle $v \in V$. Es folgt $U \leq V \leq \mathrm{Kern}(r)$, so dass $\mathrm{Kern}(r) \in \Xi$ gilt, da Ξ ja ein duales Ideal ist. Folglich ist $r \in R$, so dass die Folgerung des Dichtesatzes für R gilt. Hieraus folgt insbesondere, dass M ein irreduzibler Rechtsmodul über R ist.

Es sei H eine Hyperebene, die zu Ξ gehört. Ferner sei $0 \neq x \in O(H)$ sowie $y \in O(H)$. Ferner sei $u \in M - H$. Setze $v := ux$ und $w := uy$. Weil die Folgerung des Dichtesatzes für R gilt, gibt es ein $r \in R$ mit $vr = w$. Es folgt $u(xr - y) = 0$. Wegen $M = Ku \oplus H$ ist daher $xr = y$ und folglich $O(H) = xR$, so dass $O(H)$ ein minimales Rechtsideal von R ist, für das überdies $O(H)R = O(H)$ gilt.

Es sei $r \in R$. Setze $U := \mathrm{Kern}(r)$. Weil Ξ ein duales Ideal ist, gibt es dann Hyperebenen $H_1, \ldots, H_n \in \Xi$ mit $U = \bigcap_{i:=1}^n H_i$. Es folgt

$$r \in O(U) = \sum_{i:=1}^{n} O(H_i),$$

so dass R Summe von minimalen Rechtsidealen ist. Also ist R vollständig reduzibel.

Es seien nun H und H' zwei verschiedene Hyperebenen, die beide zu Ξ gehören. Es sei P ein Punkt auf H, der nicht auf H' liegt, und Q ein Punkt auf H', der nicht auf H liegt. Es sei $P = Kp$ und $Q = Kq$. Schließlich sei $S := K(p + q)$. Es gibt dann einen Endomorphismus r von M mit $pr = q$, $qr = p$ und $\mathrm{Kern}(r) = H \cap H'$. Weil Ξ ein duales Ideal ist, ist $\mathrm{Kern}(r) \in \Xi$, so dass $r \in R$ gilt. Es sei weiter π die Projektion von M auf S mit $\mathrm{Kern}(\pi) = H$ und π' die Projektion von M auf S mit $\mathrm{Kern}(\pi')H'$. Es folgen die Gleichungen

$$\begin{aligned} qr\pi r &= p\pi r = 0 = q\pi', \\ (p+q)r\pi r &= p + q = (p+q)\pi', \\ ur\pi r &= 0 = u\pi' \end{aligned}$$

für alle $u \in H \cap H'$. Daher ist $r\pi r = \pi'$. Definiert man nun die Abbildung λ durch $\lambda(\pi s) := r\pi s$, so ist λ ein Homomorphismus von $O(H) = \pi R$ auf $r\pi R$. Wegen $r\pi r = \pi' \in r\pi R \cap O(H')$ ist λ also ein Isomorphismus von $O(H)$ auf $O(H')$. Hieraus folgt insbesondere, dass R homogen ist.

Die Ideale der Form $O(H)$ mit einer Hyperebene $H \in \Xi$ sind aber alle minimalen Rechtsideale von R. Ist nämlich I ein minimales Rechtsideal und ist H eine Hyperebene in ξ, so gibt es, da R homogen ist, einen Isomorphismus λ von $O(H)$ auf I. Wie wir bereits gesehen haben, wird $O(H)$ von einem Idempotent π erzeugt. Setze $r := \lambda(\pi)$. Dann ist $r = r\pi \in I \cap rR$. Wegen der Minimalität von I ist daher $I \subseteq rR$, so dass $I = rR$ ist. Wegen $r \in O(\mathrm{Kern}(r))$ gilt weiter $I \subseteq O(\mathrm{Kern}(r))$. Weil der Rang von π gleich 1 und $r \neq 0$ ist, ist 1 auch der Rang von r. Folglich ist $\mathrm{Kern}(r)$ eine Hyperebene. Somit ist $O(\mathrm{Kern}(r))$ ein minimales Rechtsideal und folglich $I = O(\mathrm{Kern}(r))$.

Weil nun alle minimalen Rechtsideale Idempotente enthalten, ist ihr Quadrat niemals das Nullideal. Daher ist das Jacobson-Radikal von R gleich dem Nullideal, so dass R einfach ist. Hieraus folgt schließlich, dass M auch ein treuer R-Modul ist.

6.14. Satz. *Es sei R ein einfacher, vollständig reduzibler Ring und M sei ein treuer, irreduzibler R-Rechtsmodul. Setze $K := \mathrm{End}_R(M)$. Ist L ein Linksideal*

von R, so setzen wir

$$\Psi(L) := \sum_{\sigma \in L} M\sigma.$$

Ist $U \in L^K(M)$, so setzen wir

$$\Phi(U) := \{\sigma \mid \sigma \in R,\ M\sigma \leq U\}.$$

Dann ist Ψ ein Isomorphismus von $L^R(R)$ auf $L^K(M)$ und es gilt $\Psi^{-1} = \Phi$.

Beweis. Es ist trivial, dass $\Phi(U)$ ein Linksideal von R und dass $\Phi(L)$ ein Teilraum von M ist.

Es sei Ξ die Menge der Kerne der Elemente von R. Nach 6.11 ist Ξ dann ein duales Ideal von $L^K(M)$ aus Unterräumen endlichen Ko-Ranges, für das außerdem $\bigcap_{U \in \Xi} U = \{0\}$ gilt. Weil jedes $U \in \Xi$ Schnitt von Hyperebenen ist, die ebenfalls zu Ξ gehören, gilt sogar

$$\bigcap_{H \in \Xi,\ H \text{ ist Hyperebene}} H = \{0\}.$$

Ferner ist

$$R = \bigl\{r \mid r \in \mathrm{End}^K(M),\ \mathrm{Kern}(r) \in \Xi\bigr\}.$$

Es sei $U \in L^K(M)$. Dann ist

$$\Psi\Phi(U) = \Psi\bigl(\{\sigma \mid \sigma \in R,\ M\sigma \leq U\}\bigr) = \sum_{\sigma \in R, M\sigma \leq U} M\sigma \leq U.$$

Es sei P ein Punkt mit $P \leq U$. Nach der zuvor gemachten Bemerkung, dass der Schnitt über die zu Ξ gehörenden Hyperebenen Null ist, gibt es also eine Hyperebene $H \in \Xi$ mit $M = P \oplus H$. Es sei π die Projektion von M auf P mit Kern H. Dann ist $\pi \in R$ und wegen $M\pi = P \leq U$ gilt sogar $\pi \in \Phi(U)$. Folglich ist $P = M\pi \leq \Psi\Phi(U)$. Weil U die obere Grenze der in U liegenden Punkte ist, ist also $U \leq \Psi\Phi(U)$, so dass in der Tat $U = \Phi\Psi(U)$ ist.

Es sei L ein Linksideal von R. Dann ist

$$\Phi\Psi(L) = \Phi\bigl(\textstyle\sum_{\sigma \in L} M\sigma\bigr) = \{\tau \mid \tau \in R, M\tau \leq \sum_{\sigma \in L} M\sigma\} \supseteq L.$$

Es sei $\tau \in \Phi\Psi(L)$. Wir müssen zeigen, dass $\tau \in L$ ist. Nun hat $M\tau$ endlichen Rang. Wie wir weiter oben schon gesehen haben, gibt es ein $C \in \Xi$ mit $M = M\tau \oplus C$. Ist π die Projektion von M auf $M\tau$ mit $\mathrm{Kern}(\pi) = C$, so ist $\tau \in \Phi\Psi(L)$ und es gilt $\tau\pi = \tau$. Es genügt daher zu zeigen, dass $\pi \in L$ gilt. Ist $b_1, \ldots, b_n$ eine Basis von $M\tau$, so definieren wir Projektionen ρ_i durch $b_j\rho_i := 0$, für $j \neq i$ und $b_i\rho_i := b_i$ sowie $c\rho_i := 0$ für alle $c \in C$. Weil Ξ ein duales Ideal ist, liegen alle ρ_i in R und damit in $\Phi\Psi(L)$. Weil $\pi = \sum_{i:=1}^n \rho_i$ ist, dürfen wir daher annehmen, dass der Rang von π gleich 1 ist.

Es gibt nun $\sigma_1, \ldots, \sigma_t$ in L mit

$$M\pi \leq \sum_{i:=1}^t M\sigma_i.$$

Es sei $M\pi = Kp$. Ein solches p gibt es, da der Rang von π ja Eins ist. Es gibt dann $m_i \in M$ mit $p = \sum_{i:=1}^{t} m_i\sigma_i$. Es sei $0 \neq m \in M$. Dann ist $mR = M$. Es gibt daher $\lambda_i \in R$ mit $m_i = m\lambda_i$. Es folgt

$$p = m \sum_{i:=1}^{t} \lambda_i\sigma_i,$$

so dass also $p = m\sigma$ ist mit einem $\sigma \in L$. Es gibt eine Projektion $\alpha \in R$ von M auf Km. Es folgt

$$p = m\alpha\sigma,$$

so dass wir annehmen dürfen, dass σ den Rang 1 hat.

Weil der Rang von σ gleich Eins ist, ist also $\sigma, \pi \in \Psi(Kp)$. Der Ko-Rang von $U := \mathrm{Kern}(\pi) \cap \mathrm{Kern}(\sigma)$ sei gleich 2. Dann gehört U wiederum zu Ξ. Es gibt nun Elemente a_1 und a_2 mit $\mathrm{Kern}(\pi) = Ka_1 \oplus U$ und $\mathrm{Kern}(\sigma) = Ka_2 \oplus U$. Es folgt

$$M = Ka_1 \oplus Ka_2 \oplus U.$$

Wir definieren ρ durch $a_1\rho := a_2$, $a_2\rho = a_1$ und $\mathrm{Kern}(\rho) := U$. Es folgt $a_1\rho\sigma = 0$, so dass $\mathrm{Kern}(\rho\sigma) = \mathrm{Kern}(\sigma)$ ist. Es folgt weiter, dass $M\rho\sigma = Kp$ ist. Wir dürfen daher annehmen, dass der Kern von σ gleich dem Kern von π ist.

Definiere $\mu \in R$ durch $m\mu = km$ und $\mathrm{Kern}(\mu) = \mathrm{Kern}(\pi)$, wobei $k \in K$ durch $m\pi = kp$ definiert sei. Dann ist

$$m\mu\sigma = km\sigma = kp = m\pi$$

und folglich $\pi = \mu\sigma$, da die Kerne der drei Abbildungen identisch sind. Also ist $\pi = \mu\sigma \in L$, so dass in der Tat $L = \Phi\Psi(L)$ ist. Damit ist der Satz bewiesen.

Ist R ein einfacher, vollständig reduzibler Ring, so ist er auch als Linksmodul über sich vollständig reduzibel, wie der gerade bewiesene Satz zeigt. Dennoch besteht scheinbar eine Unsymmetrie zwischen dem Verband der Linksideale und dem Verband der Rechtsideale von R. Dieser Eindruck der Unsymmetrie wird noch bestärkt durch das folgende Beispiel.

Es sei M ein Linksvektorraum über dem Körper K und B sei eine Basis von M. Wir nehmen an, dass B nicht endlich sei. Es sei Ξ die Menge der Teilräume U von M, für die $B - U$ endlich ist. Dann ist Ξ ein duales Ideal von $L^K(M)$ mit $\Xi \subseteq E^K(M)$ und $\bigcap_{U \in \Xi} U = \{0\}$. Setzt man

$$R := \big\{\sigma \mid \sigma \in J^K(M),\ \mathrm{Kern}(\sigma) \in \Xi\big\},$$

so ist R nach 6.13 ein vollständig reduzibler, einfacher Ring. Dieser Ring ist nun nicht gleich $J^K(M)$. Ist nämlich $a \in B$ und definiert man ρ durch $b\rho := a$ für alle $b \in B$, so ist $\rho \in J^K(M)$ und es gilt $B \cap \mathrm{Kern}(\rho) = \{0\}$. Somit liegt ρ nicht in R.

Diese scheinbare Unsymmetrie wird aber beseitigt, wenn man neben einem irreduziblen Rechtsmodul über R einen geeigneten irreduziblen Linksmodul über R in die Betrachtungen mit einbezieht. Der Rest dieses Abschnitts sei der Darstellung dieses Sachverhalts gewidmet.

Das Rechtsideal I des Ringes R heißt *nilpotent*, wenn es eine natürliche Zahl n gibt, so dass $I^n = \{0\}$ ist. Nilpotente Linksideale, bzw. nilpotente Ideale werden entsprechend definiert.

6.15. Satz. *Es sei R ein Ring. Dann sind die folgenden Aussagen gleichbedeutend:*
a) *R enthält kein von $\{0\}$ verschiedenes nilpotentes Rechtsideal.*
b) *R enthält kein von $\{0\}$ verschiedenes nilpotentes Ideal.*
c) *R enthält kein von $\{0\}$ verschiedenes nilpotentes Linksideal.*

Beweis. Weil zweiseitige Ideale auch Rechtsideale sind, ist b) eine Konsequenz von a).

Es sei I ein nicht triviales nilpotentes Rechtsideal von R. Ist dann $RI = \{0\}$, so ist I sogar ein zweiseitiges nilpotentes Ideal von R. Es sei also $RI \neq \{0\}$ und $I^n = \{0\}$. Dann ist RI ein nicht triviales zweiseitiges Ideal von R. Wegen

$$(RI)^n = R(IR)^{n-1}I \subseteq RI^n = \{0\}$$

ist RI nilpotent. Somit ist a) eine Folge von b)

Die Äquivalenz von b) mit c) beweist sich entsprechend.

6.16. Satz. *Es sei R ein Ring ohne von $\{0\}$ verschiedene, zweiseitige Ideale. Ist e ein von 0 verschiedenes Idempotent von R, so sind die folgenden Aussagen äquivalent:*
a) *eR ist ein minimales Rechtsideal von R.*
b) *eRe ist ein Körper.*
c) *Re ist ein minimales Linksideal von R.*

Beweis. Es gelte a). Wegen $e = e^3 \in eRe$ besteht eRe nicht nur aus der Null. Weiter folgt $(ere)R = eR$, falls nur $ere \neq 0$ ist. Es gibt dann ein $s \in R$ mit $eres = e^2 = e$. Hieraus folgt weiter

$$e = e^2 = erese = ereese,$$

so dass ere ein Rechtsinverses hat. Da e eine Rechtseins von eRe ist, bilden die von Null verschiedenen Elemente von eRe eine Gruppe, so dass eRe ein Körper ist.

Es gelte b) und I sei ein von $\{0\}$ verschiedenes Rechtsideal, welches in eR enthalten ist. Weil R keine nicht trivialen, nilpotenten zweiseitigen Ideale enthält, folgt mit 6.15, dass $I^2 \neq \{0\}$ ist. Nun ist $I^2 \subseteq IeR$ und daher $IeR \neq \{0\}$. Hieraus folgt die Existenz eines $a \in I$ mit $aeR \neq \{0\}$. Wegen $I \subseteq eR$ ist $ea = a$. Es folgt

$$eae = ae = ae^2 \in IeR \subseteq I.$$

Somit ist eae ein von Null verschiedenes Element im Schnitt von I mit eRe. Weil eRe ein Körper ist, gibt es ein $b \in R$ mit $e = eaeebe$. Hieraus folgt $e \in I$ und damit $eR \subseteq I$, so dass eR in der Tat ein minimales Rechtsideal ist.

Die Äquivalenz von b) mit c) beweist sich entsprechend.

6.17. Satz. *Es sei R ein einfacher Ring und e sei ein Idempotent von R, so dass $K := eRe$ ein Körper ist. Setze $W := eR$ und $V := Re$. Dann gilt:*

a) *Es ist* $W \cap V = K$.
b) W *ist ein Links- und* V *ein Rechtsvektorraum über* K.
c) *Die Abbildung, die* $w \in W$ *und* $v \in V$ *ihr Produkt* wv *in* R *zuordnet, ist eine Koppelung von* W *mit* V *über* K.
d) *Ist* $\varphi \in \mathrm{End}_R(W)$, *so ist* $\varphi e \in K$ *und es gilt* $\varphi w = (\varphi e)w$ *für alle* $w \in W$. *Somit ist* K *zu* $\mathrm{End}_R(W)$ *isomorph.*
e) *Ist* $\varphi \in \mathrm{End}^R(V)$, *so ist* $\varphi e \in K$ *und es gilt* $v\varphi = v(\varphi e)$ *für alle* $v \in V$. *Somit ist* K *zu* $\mathrm{End}^R(V)$ *isomorph.*
f) *Für* R *gilt der Dichtesatz sowohl als Unterring von* $\mathrm{End}_K(V)$ *als auch als Unterring von* $\mathrm{End}^K(W)$.

Beweis. a) Es ist $K = eRe \subseteq Re \cap eR = W \cap V$. Ist andererseits $x \in Re \cap eR$, so ist $x = re = es$ und folglich $x = exe \in K$.

b) ist trivial.

c) Von den nachzuweisenden Bedingungen sind nur die Bedingungen 5) und 6) nicht völlig banal. Es sei also $w \in W$ und es gelte $wV = \{0\}$. Ferner sei $w = er$. Dann ist also $erse = 0$ für alle $s \in R$. Wäre $er \neq 0$, so folgte $erR = eR$, da eR wegen der Einfachheit von R nach 6.16 ein minimales Ideal ist. Es gäbe daher ein $t \in R$ mit $ert = e$. Hieraus folgte der Widerspruch $0 = erte = e$. Entsprechend zeigt man, dass aus $Wv = \{0\}$ folgt, dass $v = 0$ ist.

d) Es ist $\varphi e \in W = eR$. Hieraus folgt

$$\varphi e = \varphi(e^2) = (\varphi e)e \in eRe = K.$$

Alles weitere ist banal.

e) beweist sich wie d).

f) folgt mittels d) bzw. e), da R als einfacher Ring ja auf jedem irreduziblen Modul treu operiert, also primitiv ist.

6.18. Satz. *Es sei* R *ein einfacher, vollständig reduzibler Ring. Dann enthält* R *ein Idempotent* e, *so dass* eR *ein minimales Rechtsideal ist. Setze* $K := eRe$. *Dann ist* K *ein Körper. Setze* $W := eR$ *und* $V := Re$. *Dann sind* W *und* V *gemäß der Beschreibung von Satz 6.17 gekoppelte Vektorräume über* K. *Setze*

$$\Xi^W := \bigl\{X^\perp \mid X \in E_K(V)\bigr\}$$

und

$$\Xi_V := \bigl\{Y^\top \mid Y \in E^K(W)\bigr\}.$$

Dann gilt:
a) *Der Verband* $L^R(R)$ *der Linksideale von* R *ist isomorph zu* $L^K(W)$.
b) *Der Verband* $L_R(R)$ *der Rechtsideale von* R *ist isomorph zu* $L_K(V)$.
c) *Es ist*

$$R = \bigl\{\sigma \mid \sigma \in J^K(W),\ \mathrm{Kern}(\sigma) \in \Xi^W\bigr\}.$$

d) *Es ist*

$$R = \bigl\{\sigma \mid \sigma \in J_K(V),\ \mathrm{Kern}(\sigma) \in \Xi_V\bigr\}.$$

Beweis. a) ist nichts Anderes als die Aussage des Satzes 6.14. Sie besagt darüber hinaus, dass R auch als Linksmodul über sich vollständig reduzibel ist. Weil V ein irreduzibler Linksmodul über R ist, gilt daher auch b).

Zur Notation $E_K(V)$, $E^K(W)$ siehe 6.6 und die Bemerkung vor 5.14.

Um c) zu beweisen, sei zunächst $r \in R$. Dann hat rV endlichen Rang. Ist $w \in W$, so gilt $w(rV) = \{0\}$ genau dann, wenn $(wr)V = \{0\}$ ist. Dies ist wiederum genau dann der Fall, wenn $wr = 0$ ist. Also ist $\mathrm{Kern}(r) = (rV)^\perp$, wobei Kern sich hier auf die Wirkung von r auf W bezieht. Es gilt also $\mathrm{Kern}(r) \in \Xi^W$. Es sei $Y \in \Xi^W$. Es gibt dann einen Teilraum $X \in E_K(V)$ mit $Y = X^\perp$. Es sei $b_1, \ldots, b_n$ eine Basis von X. Auf Grund des Dichtesatzes, der nach 5.17 ja gilt, gibt es ein $r \in R$ mit $rb_i = b_i$ für alle i. Es ist $X \leq rV$ und daher $\mathrm{Kern}(r) = (rV)^\perp \leq X^\perp$. Nach 6.11 gibt es also ein $s \in R$ mit $\mathrm{Kern}(s) = X^\perp = Y$. Damit ist gezeigt, dass Ξ^W gerade die Menge der $\mathrm{Kern}(r)$ mit $r \in R$ ist. Eine nochmalige Anwendung von 6.11 zeigt dann die Gültigkeit von c).

d) gilt aus Symmetriegründen.

Was in diesem Abschnitt über das Jacobson-Radikal eines Ringes gesagt wurde, ist natürlich alles auf den uns allein interessierenden Fall vollständig reduzibler Ringe zugeschnitten worden. Der Leser, der mehr erfahren möchte, sei auf die Bücher über Ringtheorie verwiesen.

7. Endliche projektive Räume

In diesem Abschnitt wollen wir die Anzahl der Unterräume vom Range i eines endlichen projektiven Raumes sowie die Anzahl seiner Basen bestimmen. Dies bedarf noch einiger Vorbereitung. Wir beweisen zunächst den folgenden Satz.

7.1. Satz. *Es sei L ein irreduzibler projektiver Verband. Sind A, B und D Elemente von L mit der Eigenschaft, dass D maximal ist bezüglich der Eigenschaft, mit A und B trivialen Schnitt zu haben, so ist $A + D \leq B + D$ oder $B + D \leq A + D$.*

Beweis. Es sei P ein Punkt von $A + B + D$, der nicht in D liegen möge. Dann ist $A \cap (D + P) \neq 0$ oder $B \cap (D + P) \neq 0$.

Es sei etwa $A \cap (D+P) \neq 0$. Es gibt dann einen Punkt $Q \leq A \cap (D+P)$. Ist $Q = P$, so ist $P \leq A+D$. Es sei also $Q \neq P$. Nach 2.6 gibt es dann einen Punkt $R \leq D$ mit $Q \leq P + R$. Wegen $A \cap D = 0$ ist $Q \neq R$. Daher ist $P + R = Q + R$ und folglich $P \leq A + D$. Ist $B \cap (D + P) \neq 0$, so folgt entsprechend $P \leq B + D$. Also liegen die Punkte von $A + B + D$ in $A + D$ oder in $B + D$.

Gäbe es nun einen Punkt U auf $A + D$, der nicht in $B + D$ läge, und einen Punkt V auf $B + D$, der nicht in $A + D$ läge, dann gäbe es, da L ja irreduzibel ist, einen Punkt W auf $U + V$, der weder zu $A + D$ noch zu $B + D$ gehörte. Dies widerspräche aber $R \leq A + B + D$. Also ist $A + D \leq B + D$ oder $B + D \leq A + D$.

7.2. Satz. *Es sei L ein irreduzibler projektiver Verband mit dem größten Element* Π. *Sind A und B Elemente endlichen Ranges von L und gilt* $\mathrm{Rg}_L(A) = \mathrm{Rg}_L(B)$, *so gibt es ein $C \in L$ mit*

$$\Pi = A \oplus C = B \oplus C.$$

Beweis. Weil A und B endlichen Rang haben, hat auch $A+B$ endlichen Rang, so dass der Quotient $(A+B)/0$ noethersch ist. Unter allen Teilräumen von $A+B$, die mit A und B trivialen Schnitt haben, gibt es also einen maximalen Ranges. Es sei D ein solcher. Nach 7.1 ist dann oBdA $A+D \leq B+D$. Nun ist aber

$$\mathrm{Rg}_L(A+D) = \mathrm{Rg}_L(A) + \mathrm{Rg}_L(D) = \mathrm{Rg}_L(B) + \mathrm{Rg}_L(D) = \mathrm{Rg}_L(B+D),$$

so dass $A+D = B+D = A+B$ ist.

Ist nun F ein Komplement von $A+B$ in Π, so ist $C := D+F$ ein gemeinsames Komplement von A und B in Π.

7.3. Korollar. *Ist L ein irreduzibler projektiver Verband, sind A, $B \in L$ und gilt $\mathrm{Rg}_L(A) = \mathrm{Rg}_L(B) < \infty$, so sind die Quotienten Π/A und Π/B bzw. $A/0$ und $B/0$ isomorph.*

Beweis. Nach 7.2 gibt es ein gemeinsames Komplement C von A und B. Daher gilt nach der Transformationsregel

$$\begin{aligned}\Pi/A = (A+C)/A &\cong C/(A\cap C) = C/0\\ &= C/(B\cap C) \cong (B+C)/B = \Pi/B\end{aligned}$$

und

$$\begin{aligned}A/0 = A/(A\cap C) &\cong (A+C)/C\\ &= (B+C)/C \cong B/(B\cap C) = B/0,\end{aligned}$$

womit das Korollar bewiesen ist.

7.4. Satz. *Ist L ein projektiver Verband, so sind die folgenden Aussagen äquivalent:*

a) *L ist irreduzibel oder L ist isomorph zu $(P(A), \subseteq)$, wobei A die Menge der Punkte von L bezeichne.*

b) *Ist k eine natürliche Zahl mit $k \leq \mathrm{Rg}(L)$ und sind X und Y zwei Teilräume des Ranges k von L, so sind die Quotienten $X/0$ und $Y/0$ isomorph.*

c) *Sind G und H zwei Geraden von L, so sind $G/0$ und $H/0$ isomorph.*

Beweis. a) impliziert b): Ist L irreduzibel, so gilt b) nach 7.3. Ist L zu $(P(A), \subseteq)$ isomorph, so ist $|X| = k = |Y|$, so dass b) auch in diesem Falle gilt.

b) impliziert natürlich c).

c) impliziert a): Gibt es eine Gerade, die mehr als zwei Punkte trägt, so tragen alle Geraden mehr als zwei Punkte, so dass L nach 2.14 irreduzibel ist. Gibt es keine solche Gerade, so ist L nach Satz 2.15 zu dem cartesischen Produkt $\mathrm{cart}_{P\in A} P/0$ isomorph. In jedem Falle gilt also a).

Wir setzen im Folgenden stets voraus, dass der projektive Verband L mindestens den Rang 2 hat und dass alle seine Geraden gleichviele Punkte tragen.

Sind G und H zwei Geraden des endlichen projektiven Verbandes L, so tragen die Geraden G und H nach unserer Annahme gleichviele Punkte. Ist $q+1$ diese Anzahl, so heißt q *Ordnung* von L. Ist L irreduzibel, so ist $q \geq 2$. Im anderen Fall ist $q = 1$.

Es sei weiterhin L endlich. Wir bezeichnen mit $N_i(k, L)$ die Anzahl der Teilräume des Ranges i, die in einem Teilraum des Ranges k von L enthalten sind. Mit 7.4 folgt auf Grund unserer Annahme über die Gleichmächtigkeit der Geraden von L, dass diese Zahl wirklich nur von i und k abhängt, nicht jedoch von der speziellen Auswahl des Unterraumes des Ranges k. Offenbar gilt $N_0(1, L) = 1 = N_1(1, L)$. Weiter gilt

7.5. Satz. *Es sei L ein endlicher projektiver Verband des Ranges r, dessen Geraden alle gleichviele Punkte tragen. Ist $0 \leq i \leq j \leq n \leq r$, so ist*

$$N_i(n, L)N_{j-i}(n - i, L) = N_i(j, L)N_j(n, L).$$

Beweis. Wie wir schon festgestellt haben, hängen die fraglichen Zahlen alle nur von den angegebenen Parametern ab. Es sei nun U ein Unterraum des Ranges n von L. Ferner sei I die Menge der Paare (A, B) von Unterräumen A und B mit $\mathrm{Rg}_L(A) = i$, $\mathrm{Rg}_L(B) = j$ und $A \leq B \leq U$. Die Anzahl der B vom Range j, die ein gegebenes A vom Range i umfassen und gleichzeitig in U liegen, ist gleich der Anzahl der Teilräume des Ranges $j - i$ des Quotienten U/A. Ist C ein Komplement von A in U, so gilt nach der Transformationsregel $U/A \cong C/0$. Daher ist diese Anzahl gleich $N_{j-i}(n - i, L)$. Also ist

$$|\,\mathrm{I}\,| = N_i(n, L)N_{j-i}(n - i, L).$$

Andererseits ist $N_i(j, L)$ die Anzahl der Teilräume vom Range i, die in einem gegebenen Teilraum des Ranges j enthalten sind. Analoges gilt für $N_j(n, L)$. Daher ist

$$|\,\mathrm{I}\,| = N_i(j, L)N_j(n, L),$$

so dass der Satz bewiesen ist.

Es sei q eine natürliche Zahl. Wir definieren die q-Analoga der Fakultäten durch $(0, q)! := 1$ und

$$(n + 1, q)! := (n, q)! \sum_{i:=0}^{n} q^i$$

für $n \geq 0$. Ist $q = 1$, so ist $(n, q)! = n!$.

Sind k und n nicht negative ganze Zahlen und gilt $k \leq n$, ist ferner q eine natürliche Zahl, so setzen wir

$$\binom{n}{k, q} := \frac{(n, q)!}{(k, q)!(n - k, q)!}.$$

Ist $q = 1$, so sind dies die Binomialkoeffizienten. Ist $q > 1$, so heißen diese Zahlen *gaußsche Zahlen*.

Ist $q > 1$, so gilt

$$\binom{n}{k, q} = \prod_{i:=1}^{k} \frac{q^{n+1-i} - 1}{q^i - 1}.$$

Diese Darstellung ist für das Auge gefälliger.

7.6. Satz. *Es sei L ein endlicher projektiver Verband, dessen Geraden alle gleichviele Punkte tragen. Es sei q die Ordnung und r der Rang von L. Sind dann k und n nicht negative ganze Zahlen mit $k \leq n \leq r$, so gilt*

$$N_k(n, L) = \binom{n}{k, q}.$$

Insbesondere hängen die Zahlen $N_k(r, L)$ also nur von k, r und q ab.

Beweis. Nach 7.4 sind auf Grund unserer Annahme alle Unterräume gegebenen Ranges von L isomorph. Ist U ein Unterraum des Ranges n und ist P ein Punkt von U, so ist die Anzahl der Geraden durch P, die in U liegen, gleich der Anzahl der Unterräume des Ranges 1 in U/P. Ist $U = P \oplus C$, so folgt mittels der Transformationsregel, dass diese Anzahl gleich der Anzahl der Punkte auf C, dh., dass sie gleich $N_1(n-1, L)$ ist. Auf jeder Geraden durch P liegen q Punkte, die von P verschieden sind, und je zwei dieser Geraden haben nur P gemeinsam. Da schließlich jeder Punkt von U mit P durch eine Gerade verbunden ist, ist

$$N_1(n, L) = qN_1(n-1, L) + 1.$$

Weil $N_1(1, L) = 1$ ist, folgt mittels Induktion, dass

$$N_1(n, L) = \textstyle\sum_{i:=0}^{n-1} q^i = \binom{n}{1,q}$$

ist. Setzt man in 7.5 nun $i := 1$ und $j := k$, so folgt

$$(\textstyle\sum_{i:=0}^{n-1} q^i) N_{k-1}(n-1, L) = (\sum_{i:=0}^{k-1} q^i) N_k(n, L).$$

Vollständige Induktion liefert nun das gewünschte Ergebnis.

Der soeben bewiesene Satz besagt unter anderem, dass die Binomialkoeffizienten wie auch die gaußschen Zahlen natürliche Zahlen sind, letztere zumindest für solche q, die Ordnung eines endlichen projektiven Raumes sind, was nicht für alle natürlichen Zahlen zutrifft. Es ist jedoch eine einfache Übungsaufgabe zu zeigen, dass diese einschränkende Voraussetzung an q nicht gemacht werden muss. Für die gaußschen Zahlen gilt nämlich die Funktionalgleichung

$$\binom{n+1}{k, q} = q\binom{n}{k, q} + \binom{n}{k-1, q}.$$

7.7. Satz. *Es sei L ein endlicher projektiver Verband des Ranges r, dessen Geraden alle gleichviele Punkte tragen. Ist $0 \leq k \leq r$, so ist*

$$N_k(r, L) = N_{r-k}(r, L).$$

Beweis. Weil alle Geraden von L gleichviele Punkte tragen, ist L nach 7.4 irreduzibel oder aber zum Potenzmengenverband einer geeigneten Menge isomorph. Weil L endlich ist, ist im ersten Fall L^d nach Früherem projektiv. Im zweiten Fall ist L^d ebenfalls projektiv. Die Komplementbildung vermittelt ja

einen Isomorphismus des Potenzmengenverbandes auf seinen dualen Verband. Wir dürfen daher im Folgenden L^d in unserer Argumentation verwenden.

Es sei nun G eine Gerade von L und H sei ein Komplement von G in Π. Dann ist H eine Gerade von L^d. Aus der Isomorphie von $G/0$ und Π/H folgt daher, dass L und L^d die gleiche Ordnung haben. Da diese Verbände nach 5.9 den gleichen Rang haben und die Unterräume vom Ko-Rang $r-k$ von L gerade die Unterräume vom Range k von L^d sind, folgt mit 7.6

$$N_k(r, L) = N_k(r, L^d) = N_{r-k}(r, L).$$

Wir werden später sehen, dass q im Falle $r \geq 4$ stets Potenz einer Primzahl ist. Im Falle $r = 3$, dh. im Falle, dass L eine projektive Ebene ist, ist das eine bislang unbewiesene Vermutung. Man weiß nach einem Satz von Bruck und Ryser, dass eine Zahl q, die kongruent 1 oder 2 modulo 4 ist und die sich nicht als Summe von zwei Quadraten darstellen lässt, niemals die Ordnung einer endlichen projektiven Ebene ist.

7.8. Satz. *Ist L ein endlicher, irreduzibler projektiver Verband der Ordnung q und des Ranges r, so ist die Anzahl $A_S(r, q)$ von geordneten s-Tupeln unabhängiger Punkte gleich*

$$(q-1)^{-s} q^{\frac{1}{2}s(s-1)} \prod_{i:=r+1-s}^{r} (q^i - 1).$$

Insbesondere ist die Anzahl der geordneten Basen von L gleich

$$(q-1)^{-r} q^{\frac{1}{2}r(r-1)} \prod_{i:=1}^{r} (q^i - 1).$$

Beweis. Es ist $A_1(r, q) = N_1(r, q) = (q-1)^{-1}(q^r - 1)$. Es sei bereits bewiesen, dass $A_s(r, q)$ die angegebene Form hat. Es sei $(P_1, \ldots, P_s)$ ein unabhängiges s-Tupel von Punkten. Dann ist das $(s+1)-$Tupel $(P_1, \ldots, P_s, Q)$ genau dann unabhängig, wenn $Q \not\leq \sum_{i:=1}^{s} P_i$ gilt. Somit ist die Anzahl dieser $(s+1)$-Tupel gleich

$$N_1(r, q) - N_1(s, q).$$

Folglich ist

$$A_{s+1}(r, q) = A_s(r, q)(N_1(r, q) - N_1(s, q)).$$

Hieraus folgt mit einer simplen Rechnung die Behauptung.

Es sei L ein projektiver Verband des Ranges r. Sind $P_1, \ldots, P_{r+1}$ Punkte von L mit der Eigenschaft, dass je r von ihnen unabhängig sind, also eine Basis von L bilden, so heißt $(P_1, \ldots, P_{r+1})$ *Rahmen* von L.

7.9. Satz. *Ist L ein endlicher irreduzibler projektiver Verband des Ranges r und der Ordnung q, so ist die Anzahl der Rahmen von L gleich*

$$q^{\frac{1}{2}r(r-1)} \prod_{i:=2}^{r} (q^i - 1).$$

Beweis. Es sei $P_1, \ldots, P_r$ eine Basis. Dann ist die Anzahl der Rahmen $(P_1, \ldots, P_r, X)$ gleich $(q-1)^{r-1}$: Dies ist sicherlich richtig, falls $r = 2$ ist, da in diesem Falle jedes Punktetripel ein Rahmen ist. Es sei nun $r > 2$. Es ist eine einfache Übungsaufgabe zu zeigen, dass $(P_1, \ldots, P_r, X)$ genau dann ein Rahmen ist, wenn $P_r \neq X$ und $X \not\leq \sum_{i:=1}^{r-1} P_i$ ist und wenn $(P_1, \ldots, P_{r-1}, X')$ mit $X' := (P_r + X) \cap \sum_{i:=1}^{r-1} P_i$ ein Rahmen von $\sum_{i:=1}^{r-1} P_i/0$ ist. Hieraus folgt, dass die Anzahl der Rahmen $(P_1, \ldots, P_r, X)$ gleich $q-1$ mal der Anzahl der Rahmen $(P_1, \ldots, P_{r-1}, X')$, dh., gleich $(q-1)^{r-1}$ ist. Somit ist die Anzahl der Rahmen von L gleich $(q-1)^{r-1} A_r(r, q)$. Hieraus folgt mit 7.7 die Behauptung des Satzes.

8. Kollineationen und Korrelationen

In Abschnitt 1 hatten wir den Begriff des Isomorphismus einer projektiven Geometrie auf eine andere definiert und in Abschnitt 2 den des Isomorphismus zwischen zwei Verbänden. Dass es bei projektiven Geometrien nicht darauf ankommt, welchen der beiden Isomorphiebegriffe man der Theorie zu Grunde legt, zeigt der folgende Satz.

8.1. Satz. *Es seien L und L' zwei projektive Verbände, es sei Σ die projektive Geometrie aus den Punkten und Geraden von L und Σ' die projektive Geometrie aus den Punkten und Geraden von L'. Ist nun σ ein Isomorphismus von Σ auf Σ', so gibt es genau einen Isomorphismus τ von L auf L' mit $P^\sigma = P^\tau$ und $G^\sigma = G^\tau$ für alle Punkte P und alle Geraden G von Σ. Ist umgekehrt τ ein Isomorphismus von L auf L' und definiert man σ durch $P^\sigma := P^\tau$ und $G^\sigma := G^\tau$ für alle Punkte P und alle Geraden G von Σ, so ist σ ein Isomorphismus von Σ auf Σ'.*

Beweis. Es sei $U \in L$ und $S(U)$ bezeichne wieder die Menge der in U enthaltenen Atome. Dann ist, wie wir wissen, $U = \sum_{P \in S(M)} P$. Wir definieren τ durch $U^\tau := \sum_{P \in S(M)} P^\sigma$. Dann ist τ eine inklusionstreue Abbildung von L in L'.

Es sei $V \in L'$. Wir setzen

$$A := \{P \mid P \in S(\Pi), P^\sigma \in S(V)\} \quad \text{und} \quad U := \sum_{P \in A} P.$$

Dann ist $A \subseteq S(U)$ und folglich $V \leq U^\tau$. Wir zeigen, dass $V = U^\tau$ ist, indem wir zeigen, dass $A = S(U)$ gilt. Dazu sei Q ein Punkt von U. Es gibt dann endlich viele Punkte $P_1, \ldots, P_n \in A$ mit $Q \leq \sum_{i:=1}^n P_i$. Ist $Q = P_1$, so ist $Q \in A$. Wir dürfen daher annehmen, dass Q von P_1 verschieden ist. Wegen $Q \leq P_1 + \sum_{i:=2}^n P_i$ gibt es nach 2.6 einen Punkt R in $\sum_{i:=2}^n P_i$ mit $Q \leq P_1 + R$. Nach Induktionsannahme ist $R \in A$, so dass wir $R = P_2$ annehmen dürfen. Weil σ ein Isomorphismus ist, ist Q^σ ein Punkt auf $P_1^\sigma + P_2^\sigma$. Weil Letzteres eine Gerade von V ist, ist Q^σ ein Punkt von V, so dass $Q \in A$ gilt. Also ist $A = S(U)$ und damit $U^\tau = V$. Folglich ist τ surjektiv. Weil σ injektiv und L relativ atomar ist, ist aber auch τ injektiv. Somit ist τ eine inklusionstreue Bijektion von L auf L'. Wendet man die gerade ausgeführte Argumentation auf

σ^{-1} an, so sieht man, dass auch τ^{-1} inklusionstreu ist, so dass τ in der Tat ein Isomorphismus von L auf L' ist.

Die Einzigkeit von τ ist banal, wie auch die zweite Aussage des Satzes.

Sind L und L' projektive Verbände und ist σ ein Isomorphismus von L auf L'^d, so heißt σ *Antiisomorphismus* von L auf L'. Nach 8.1 kann ein Antiisomorphismus σ auch dadurch beschrieben werden, dass σ eine Bijektion der Menge der Punkte von L auf die Menge der Hyperebenen von L' ist, so dass drei Punkte P, Q und R von L genau dann kollinear sind, wenn der Schnitt der Hyperebenen P^σ, Q^σ und R^σ einen Unterraum vom Ko-Rang 2 enthält, wenn also die Hyperebenen P^σ, Q^σ und R^σ so zueinander liegen wie die Blätter eines Buches. — So beschrieb E. Witt diese Situation einmal in einem Telefongespräch mit mir.

Ein Antiisomorphismus von L auf sich heißt *Korrelation*, und eine involutorische Korrelation heißt *Polarität*.

Es sei L ein projektiver Verband und $\mathrm{UR}_r(L)$ bezeichne die Menge der Unterräume vom Range r von L. Ein Isomorphismus von L auf L' bildet unabhängige Punktmengen auf unabhängige Punktmengen ab. Daher induziert jeder Isomorphismus von L auf L' eine bijektive Abbildung von $\mathrm{UR}_r(L)$ auf $\mathrm{UR}_r(L')$. Dies ist besonders dann interessant, wenn r endlich ist. Ist $\mathrm{Rg}(L) = n$ endlich und ist σ ein Antiisomorphismus von L auf L', so induziert σ eine Bijektion von $\mathrm{UR}_r(L)$ auf $\mathrm{UR}_{n-r}(L')$. Wir werden nun die Frage beantworten, wie die von Isomorphismen bzw. Antiisomorphismen induzierten Abbildungen von $\mathrm{UR}_r(L)$ auf $\mathrm{UR}_s(L')$ gekennzeichnet werden können.

Es sei r eine natürliche Zahl. Sind $X, Y \in \mathrm{UR}_r(L)$ und ist $\mathrm{Rg}_L(X+Y) = r+a$, so nennen wir a den *Abstand* von X und Y. Nach 3.7 gilt

$$\mathrm{Rg}_L(X+Y) + \mathrm{Rg}_L(X \cap Y) = \mathrm{Rg}_L(X) + \mathrm{Rg}_L(Y) = 2r.$$

Also ist $\mathrm{Rg}_L(X \cap Y) = r - a$, falls a der Abstand von X und Y ist. Man nennt X und Y *benachbart*, falls X und Y den Abstand 1 haben. Eine Menge $M \subseteq \mathrm{UR}_r(L)$ von paarweise benachbarten Unterräumen heißt *maximal*, wenn aus $M \subseteq M' \subseteq \mathrm{UR}_r(L)$ und der Eigenschaft, dass die Elemente aus M' paarweise benachbart sind, $M = M'$ folgt. Diese maximalen Mengen lassen sich nun wie folgt kennzeichnen.

8.2. Satz. *Es sei L ein projektiver Verband. Ferner sei r eine natürliche Zahl mit $2 \leq r+1 \leq \mathrm{Rg}(L)$. Ist $M \subseteq \mathrm{UR}_r(L)$ eine maximale Menge von paarweise benachbarten Unterräumen, so gibt es entweder einen Unterraum U vom Range $r-1$ mit*

$$M = \{X \mid X \in \mathrm{UR}_r(L),\ U \leq X\}$$

oder einen Unterraum W vom Range $r+1$ mit

$$M = \{X \mid X \in \mathrm{UR}_r(L),\ X \leq W\}.$$

Die beiden Fälle schließen sich gegenseitig aus, falls $\mathrm{Rg}(L) > 2$ ist.

Beweis. Es seien X, Y, Z drei verschiedene Elemente aus M. Ferner sei $Z \nleq X + Y$. Dann ist

$$\mathrm{Rg}_L\big(Z \cap (X+Y)\big) \leq r - 1.$$

Andererseits ist

$$Z \cap X \leq Z \cap (X+Y)$$

und

$$Z \cap Y \leq Z \cap (X+Y).$$

Weil die Ränge der links stehenden Räume gleich $r-1$ sind, folgt $Z \cap X = Z \cap Y = Z \cap (X+Y)$. Hieraus folgt weiter $Z \cap X \cap Y = Z \cap X$. Daher ist

$$\mathrm{Rg}_L(Z \cap X \cap Y) = r - 1 = \mathrm{Rg}_L(X \cap Y).$$

Dies hat $X \cap Y \leq Z$ zur Folge.

Es sei S ein viertes Element aus M. Ist $S \nleq X + Y$, so ist $X \cap Y \leq S$, wie wir gerade gesehen haben. Es sei also $S \leq X + Y$. Dann ist $S + X = X + Y$, da S und X, bzw., X und Y ja benachbart sind. Andererseits ist $X + Y \neq X + Z$ und daher $X = (X+Y) \cap (X+Z)$. Folglich ist $S \nleq X + Z$. Nach dem bereits Bewiesenen ist daher $X \cap Y = X \cap Z \leq S$. Damit ist gezeigt, dass entweder alle Elemente von M unterhalb $X + Y$ oder dass alle Elemente von M oberhalb von $X \cap Y$ liegen. Aus der Maximalität von M folgt damit die erste Behauptung des Satzes.

Um die zweite Behauptung zu beweisen, nehmen wir an, dass

$$M = \{Z \mid Z \in L, X \cap Y < Z < X + Y\}$$

gilt. Es sei P ein Punkt, der nicht in $X \cap Y$ liege. Aus der Maximalität von M folgt, dass $(X \cap Y) + P \in M$ ist. Dann ist aber

$$P \leq (X \cap Y) + P \leq X + Y.$$

Es folgt, dass $X + Y = \Pi$ ist. Andererseits folgt aus der Maximalität von M, dass jeder Teilraum des Ko-Ranges 1 in $X + Y$ zu M gehört. Hieraus folgt $X \cap Y = 0$, so dass $r - 1 = 0$ ist. Somit ist $\mathrm{Rg}(L) = 2$. Damit ist dann alles bewiesen.

8.3. Satz. *Es sei L ein projektiver Verband und r sei eine natürliche Zahl. Sind $X, Y \in \mathrm{UR}_r(L)$ und ist a der Abstand von X und Y, so gibt es $X_0, \ldots, X_a \in \mathrm{UR}_r(L)$ mit $X = X_0$ und $X_a = Y$, so dass X_i und X_{i+1} für $i := 0, \ldots, a-1$ benachbart sind.*

Sind umgekehrt $Y_0, \ldots, Y_n \in \mathrm{UR}_r(L)$, ist $X = Y_0$ und $Y_n = Y$ und sind Y_i und Y_{i+1} für alle in Frage kommenden i benachbart, so ist $a \leq n$.

Beweis. Dies ist sicherlich richtig, falls $a \leq 1$ ist. Es sei also $a \geq 2$. Es sei P ein Punkt von X, der nicht in Y liegt. Dann ist

$$\mathrm{Rg}_L\big(P + (X \cap Y)\big) = 1 + \mathrm{Rg}_L(X \cap Y) = r - a + 1.$$

Weil $X \cap Y$ den Ko-Rang a hat, gibt es einen Teilraum Q von Y des Ranges $a - 1$ mit $X \cap Y \cap Q = \{0\}$. Setze

$$Z := P + (X \cap Y) + Q.$$

Dann ist der Rang von Z gleich r. Mit Hilfe des modularen Gesetzes folgt ferner

$$Z \cap X = P + (X \cap Y)$$

und

$$Z \cap Y = (X \cap Y) + Q.$$

Somit ist

$$\mathrm{Rg}_L(Z \cap X) = r - a + 1$$

und

$$\mathrm{Rg}_L(Z \cap Y) = r - 1.$$

Hieraus folgt mittels Induktion die erste Behauptung.

Die zweite Aussage gilt sicherlich, falls $n \leq 1$. Es sei also $n \geq 2$. Ferner sei b der Abstand von X und Y_{n-1}. Nach Induktionsannahme ist dann $b \leq n - 1$, so dass wir $b < a$ annehmen dürfen. Nun ist

$$\mathrm{Rg}_L\big((X \cap Y) + (Y_{n-1} \cap Y)\big) = 2r - a - 1 - \mathrm{Rg}_L(X \cap Y \cap Y_{n-1}).$$

Andererseits ist

$$\mathrm{Rg}_L\big((X \cap Y_{n-1}) + (Y_{n-1} \cap Y)\big) = 2r - b - 1 - \mathrm{Rg}_L(X \cap Y \cap Y_{n-1}).$$

Nun ist

$$Y_{n-1} \cap Y \leq (X \cap Y) + (Y_{n-1} \cap Y) \leq Y$$

und

$$Y_{n-1} \cap Y \leq (X \cap Y_{n-1}) + (Y_{n-1} \cap Y) \leq Y_{n-1}.$$

Daher gilt

$$r - 1 \leq \mathrm{Rg}_L\big((X \cap Y) + (Y_{n-1} \cap Y)\big) \leq r$$

und

$$r - 1 \leq \mathrm{Rg}_L\big((X \cap Y_{n-1}) + (Y_{n-1} \cap Y)\big) \leq r.$$

Wegen $b < a$ ist daher

$$\mathrm{Rg}_L\big((X \cap Y) + (Y_{n-1} \cap Y)\big) = r - 1$$

und

$$\mathrm{Rg}_L\big((X \cap Y_{n-1}) + (Y_{n-1} \cap Y)\big) = r.$$

Somit ist $a = b + 1$ und folglich $a \leq n$. Damit ist alles bewiesen.

Ist σ ein Isomorphismus des projektiven Verbandes L auf den projektiven Verband L', so induziert σ eine Bijektion von $\mathrm{UR}_r(L)$ auf $\mathrm{UR}_r(L')$ mit der Eigenschaft, dass X, $Y \in \mathrm{UR}_r(L)$ genau dann benachbart sind, wenn X^σ und

Y^σ benachbart sind. Da zwei verschiedene Punkte, bzw. zwei verschiedene Hyperebenen stets benachbart sind, hat im Falle $r = 1$ oder $r + 1 = \mathrm{Rg}(L)$ jede Bijektion von $\mathrm{UR}_r(L)$ auf $\mathrm{UR}_r(L')$ die Eigenschaft, die Nachbarschaft zu erhalten. Dies zeigt, dass die Annahme über r im Folgenden, im Wesentlichen von W. L. Chow stammenden Satz wirklich nötig ist (Chow 1949). Chow setzte von Anfang an voraus, dass $r = s$ sei.

8.4. Satz. *Sind L und L' projektive Verbände, sind r und s natürliche Zahlen und ist $2 < r+1 < \mathrm{Rg}(L)$, ist ferner σ eine Bijektion von $\mathrm{UR}_r(L)$ auf $\mathrm{UR}_s(L')$ mit der Eigenschaft, dass X, $Y \in \mathrm{UR}_r(L)$ genau dann benachbart sind, wenn X^σ und Y^σ benachbart sind, so wird σ entweder durch einen Isomorphismus von L auf L' induziert, in welchen Falle $r = s$ ist, oder aber σ wird durch einen Antiisomorphismus von L auf L' induziert, in welchem Falle $r + s = \mathrm{Rg}(L)$ ist. Die beiden Fälle schließen sich gegenseitig aus. Überdies gilt, dass der σ induzierende Isomorphismus bzw. Antiisomorphismus eindeutig bestimmt ist.*

Beweis. Es sei σ eine Bijektion von $\mathrm{UR}_r(L)$ auf $\mathrm{UR}_s(L')$, so dass X, $Y \in \mathrm{UR}_r(L)$ genau dann benachbart sind, wenn X^σ und Y^σ es sind. Dann ist auch σ^{-1} eine nachbarschaftserhaltende Abbildung von $\mathrm{UR}_s(L')$ auf $\mathrm{UR}_r(L)$. Daher bildet σ maximale Mengen von paarweise benachbarten Unterräumen wieder auf solche ab und jede maximale Menge von paarweise benachbarten Räumen aus $\mathrm{UR}_s(L')$ ist Bild einer ebensolchen aus $\mathrm{UR}_r(L)$.

Es sei $U \in \mathrm{UR}_{r-1}$ und $M := \{X \mid X \in \mathrm{UR}_r(L), U \leq X\}$. Es gibt dann nach 8.2 genau ein $U' \in \mathrm{UR}_{s-1}(L') \cup \mathrm{UR}_{s+1}(L')$ mit

$$M^\sigma = \bigl\{X' \mid X' \in \mathrm{UR}_s(L'),\ U' \leq X'\bigr\}$$

oder

$$M^\sigma = \bigl\{X' \mid X' \in \mathrm{UR}_s(L'),\ X' \leq U'\bigr\}.$$

Ist $U \in \mathrm{UR}_{r+1}(L)$, so findet man zu $M := \{X \mid X \in \mathrm{UR}_r(L), X \leq U\}$ ebenfalls genau ein $U' \in \mathrm{UR}_{s-1}(L') \cup \mathrm{UR}_{s+1}(L')$ mit

$$M^\sigma = \bigl\{X' \mid X' \in \mathrm{UR}_s(L'),\ U' \leq X'\bigr\}$$

oder

$$M^\sigma = \bigl\{X' \mid X' \in \mathrm{UR}_s(L'),\ X' \leq U'\bigr\}.$$

In beiden Fällen setzen wir $U^\sigma := U'$. Dann ist σ nach der zuvor gemachten Bemerkung eine Bijektion von

$$\mathrm{UR}_{r-1}(L) \cup \mathrm{UR}_r(L) \cup \mathrm{UR}_{r+1}(L)$$

auf

$$\mathrm{UR}_{s-1}(L') \cup \mathrm{UR}_s(L') \cup \mathrm{UR}_{s+1}(L').$$

Wegen $\mathrm{UR}_r(L)^\sigma = \mathrm{UR}_s(L')$ gilt

$$\bigl(\mathrm{UR}_{r-1}(L) \cup \mathrm{UR}_{r+1}(L)\bigr)^\sigma = \mathrm{UR}_{s-1}(L') \cup \mathrm{UR}_{s+1}(L').$$

Angenommen es seien X, $Y \in \mathrm{UR}_{r-1}(L)$ und es gelte $X^\sigma \in \mathrm{UR}_{s-1}(L')$ und $Y^\sigma \in \mathrm{UR}_{s+1}(L')$. Nach 8.3 gibt es endlich viele $X_i \in \mathrm{UR}_{r-1}(L)$ mit $X = X_0$ und $Y = X_n$, so dass X_i und X_{i+1} benachbart sind. Es gibt dann ein i, so dass $X_i^\sigma \in \mathrm{UR}_{s-1}(L')$ und $X_{i+1}^\sigma \in \mathrm{UR}_{s+1}(L')$ gilt. Wir dürfen daher annehmen, dass X und Y benachbart sind.

Es sei M die Menge der Unterräume des Ranges r, die X enthalten. Auf Grund der Definition von X^σ ist dann

$$M^\sigma = \{X' \mid X' \in \mathrm{UR}_s(L'),\ X^\sigma \leq X'\}.$$

Ist N die Menge der Unterräume des Ranges r, die Y enthalten, so folgt entsprechend

$$N^\sigma = \{Y' \mid Y' \in \mathrm{UR}_s(L'),\ Y' \leq Y^\sigma\}.$$

Ist nun $X^\sigma < Z' < Y^\sigma$, so gibt es ein $Z \in M \cap N$ mit $Z^\sigma = Z'$. Nun ist aber $M \cap N = \{X + Y\}$, so dass es zwischen X^σ und Y^σ genau einen Unterraum des Ranges s gibt. Dies widerspricht aber der relativen Atomarität des Verbandes L'. Also ist doch $\mathrm{Rg}_{L'}(X^\sigma) = \mathrm{Rg}_{L'}(Y^\sigma)$, falls nur X, $Y \in \mathrm{UR}_{r-1}(L)$ gilt. Ganz analog folgt auch für X, $Y \in \mathrm{UR}_{r+1}(L)$ die Gleichheit der Ränge von X^σ und Y^σ. Es sind also die folgenden beiden Fälle zu betrachten:

1. $\mathrm{UR}_{r-1}(L)^\sigma = \mathrm{UR}_{s-1}(L')$ und $\mathrm{UR}_{r+1}(L)^\sigma = \mathrm{UR}_{s+1}(L')$.
2. $\mathrm{UR}_{r-1}(L)^\sigma = \mathrm{UR}_{s+1}(L')$ und $\mathrm{UR}_{r+1}(L)^\sigma = \mathrm{UR}_{s-1}(L')$.

Wegen $2 < r+1 < \mathrm{Rg}(L)$ enthalten $\mathrm{UR}_{r-1}(L)$ und $\mathrm{UR}_{r+1}(L)$ je mindestens zwei Elemente. Daher gilt dies auch für $\mathrm{UR}_{s-1}(L)$ und $\mathrm{UR}_{s+1}(L')$, so dass auch $2 < s+1 < \mathrm{Rg}(L')$ gilt.

1. Fall. Hier gilt: Sind $X, Y \in \mathrm{UR}_{r-1}(L) \cup \mathrm{UR}_r(L) \cup \mathrm{UR}_{r+1}(L)$, so ist genau dann $X \leq Y$, wenn $X^\sigma \leq Y^\sigma$ ist. Insbesondere folgt, dass zwei Unterräume des Ranges $r-1$ von L genau dann benachbart sind, wenn ihre Bilder es sind.

Es sei $r = 2$. Unter Zuhilfenahme von σ^{-1} folgt, dass in diesem Falle auch $s = 2$ ist. Daher bildet σ Punkte auf Punkte und Geraden auf Geraden unter Erhaltung der Inzidenz ab. Nach 8.1 wird σ folglich von einem Isomorphismus von L auf L' induziert. Vollständige Induktion führt nun zum Ziel.

2. Fall. In diesem Falle gilt: sind $X, Y \in \mathrm{UR}_{r-1}(L) \cup \mathrm{UR}_r(L) \cup \mathrm{UR}_{r+1}(L)$, so ist genau dann $X \leq Y$, wenn $Y^\sigma \leq X^\sigma$ ist. Benachbarte Elemente werden also auch hier auf benachbarte Elemente abgebildet. Ist nun $r = 2$, so erschließt man mit Hilfe von σ^{-1}, dass die $X' \in \mathrm{UR}_s(L')$ den Ko-Rang 2 haben. Also ist in diesem Falle $r + s = \mathrm{Rg}(L')$. Es folgt ferner, dass σ kollineare Punkte auf *konfluente* Hyperebenen abbildet. Nach 8.1 wird σ folglich von einem Antiisomorphismus induziert. Induktion führt nun auch hier zum Ziele. Wird σ durch einen Isomorphismus induziert, so liegt offensichtlich der erste Fall vor und es folgt, dass σ nicht durch einen Antiisomorphismus induziert wird. Wird σ durch einen Antiisomorphismus induziert, so folgt, dass σ nicht durch einen Isomorphismus induziert wird. Die beiden Fälle schließen sich also gegenseitig aus.

Es seien nun σ und τ zwei Isomorphismen oder zwei Antiisomorphismen von L auf L', die auf $\mathrm{UR}_r(L)$ die gleiche Abbildung induzieren. Dann ist $\sigma\tau^{-1}$ ein

Automorphismus, welcher auf $\mathrm{UR}_r(L)$ die Identität induziert. Da jeder Punkt von L sich als Schnitt von Unterräumen des Ranges r darstellen lässt, folgt, dass $\sigma\tau^{-1}$ alle Punkte von L festlässt. Daher ist $\sigma = \tau$, womit alles bewiesen ist.

Der Satz von Chow sowie 8.1 sind Beispiele dafür, dass eine Abbildung eines Teils von L auf einen Teil von L' unter gewissen Voraussetzungen durch einen Isomorphismus von L auf L' induziert wird. Zwei weitere Beispiele dieser Art werden wir noch sehen. Zuvor jedoch wollen wir zeigen, dass der Satz von Chow auch in anderen Teilen der Mathematik von Nutzen ist, indem wir nach dem Vorgange von H. Mäurer einen Satz von H. Wielandt beweisen.

Ist X eine Menge, so bezeichnen wir mit S_X die *symmetrische Gruppe* auf X, dh., die Gruppe aller Bijektionen von X auf sich. Ferner bezeichnen wir mit A_X die *alternierende Gruppe* auf X, das ist die von allen Zyklen der Länge 3 erzeugte Untergruppe von S_X. Dann ist A_X ein Normalteiler von S_X.

8.5. Satz. *Es sei X eine Menge, die nicht genau sechs Punkte enthalte. Ist dann α ein Automorphismus von A_X, so gibt es ein $\gamma \in S_X$ mit $\alpha(\xi) = \gamma\xi\gamma^{-1}$ für alle $\xi \in A_X$.*

Beweis. Ist $|X| \leq 2$, so ist $A_X = \{1\}$ und daher nichts zu beweisen. Ist $|X| = 3$, so ist A_X zyklisch der Ordnung 3 und hat somit genau zwei Automorphismen, die beide durch innere Automorphismen der S_X induziert werden, da die S_X ja nicht abelsch ist.

Im folgenden enthalte X mindestens vier Elemente. Ist i eine natürliche Zahl, so bezeichnen wir mit Z_i die Menge der Elemente aus A_X, die Produkt von genau i disjunkten Zyklen sind, die alle die Länge 3 haben. Die Z_i sind Konjugiertenklassen von A_X, so dass α jedes Z_i auf ein Z_j abbildet. Wir zeigen zunächst, dass $\alpha(Z_1) = Z_1$ ist.

Weil die Elemente der A_5 nur die Ordnung 1, 2, 3 oder 5 haben, haben auch die Elemente aus dem Komplexprodukt Z_1Z_1 nur diese Ordnungen. Damit Z_i nicht leer ist, muss X mindestens $3i$ Elemente haben. Für $i \geq 2$ bedeutet dies auf Grund unserer Annahme über X, dass X in diesem Falle mindestens sieben Elemente enthält. Wegen

$$(123)(124)(567)(567) = (14)(23)(576)$$

enthält Z_2Z_2 daher Elemente der Ordnung 6. Ferner ist

$$(123)(456)(789)(147)(258)(369) = (159267348).$$

Hieraus folgt, dass Z_iZ_i für $i \geq 3$ stets Elemente enthält, deren Ordnung gleich 9 ist. Somit ist $\alpha(Z_1) = Z_1$.

Ist $\{a, b, c\}$ eine 3-Teilmenge von X, so sind (abc) und (acb) die einzigen Elemente aus Z_1 mit dieser Menge als Trägermenge. Ist $\alpha(abc) = (a'b'c')$, so ist $\alpha(acb) = (a'c'b')$. Daher wird durch

$$\beta\big(\{a, b, c\}\big) := \{a', b', c'\}$$

eine Abbildung auf der Menge der 3-Teilmengen von X definiert. Es seien $\{a, b, c\}$ und $\{a, b, d\}$ zwei benachbarte 3-Teilmengen von X. — Man erinnere sich: Die Potenzmenge von X ist mit der Inklusion als Teilordnung ein projektiver Verband und der Rang eines Teilraumes ist nichts anderes als seine Kardinalität. — Die von (abc) und (abd) erzeugte Untergruppe von A_X ist isomorph zur $A_{\{a,b,c,d\}}$. Es seien $\{a, b, c\}$ zwei Teilmengen des Abstandes 2. Dann ist die von (abc) und (ade) erzeugte Untergruppe von A_X isomorph zur $A_{\{a,b,c,d,e\}}$. — Es genügt zu bemerken, dass $(abc)(ade) = (abcde)$ ist. — Weil disjunkte Dreierzyklen eine abelsche Gruppe der Ordnung 9 erzeugen, erhält β daher die Nachbarschaft. Es gibt also nach dem Satz von Chow einen Automorphismus oder Antiautomorphismus γ von $P(M)$, der β induziert. Weil X aber nicht genau 6 Elemente enthält, kann γ ebenfalls nach dem Satz von Chow kein Antiautomorphismus sein. Somit ist γ, wenn man nur seine Wirkung auf die Punkte von X betrachtet, ein Element von S_X. Definiere λ durch

$$\lambda(\xi) := \gamma\xi\gamma^{-1}.$$

Dann ist $\alpha^{-1}\lambda$ ein Automorphismus von A_X, der alle Untergruppen von A_X, die von Elementen aus Z_1 erzeugt werden, invariant lässt. Setze $\mu := \alpha^{-1}\lambda$. Dann ist also $\mu(\zeta) = \zeta^{\epsilon(\zeta)}$ mit $\epsilon(\zeta) = \pm 1$ für alle $\zeta \in Z_1$.

Es ist $(123)(124) = (14)(23)$ und $(132)(124) = (134)$. Wäre nun $\mu(123) = (132)$, so folgte $\mu(124) = (142)$. Weil man nach Satz 8.3 je zwei 3-Teilmengen von X durch eine Kette benachbarter 3-Teilmengen verbinden kann, folgte weiter $\mu(abc) = (acb)$ für alle 3-Teilmengen $\{a, b, c\}$. Dann folgte aber der Widerspruch

$$\begin{aligned}(143) = \mu(134) &= \mu\big((132)(124)\big)\\ &= (132)\mu(124) = (123)(142) = (234).\end{aligned}$$

Also ist μ die Identität und daher $\alpha = \lambda$, was zu beweisen war.

Ohne Beweis sei hier mitgeteilt, dass die S_X im Falle $|X| = 6$ einen Automorphismus besitzt, der kein innerer Automorphismus ist. Weil die A_X eine charakteristische Untergruppe von S_X ist, induziert dieser Automorphismus einen Automorphismus in A_X. Dieser Automorphismus bildet Z_1 auf Z_2 ab, kann also nicht durch einen inneren Automorphismus von S_X induziert werden.

8.6. Satz. *Es seien L und L' projektive Verbände und r und s seien natürliche Zahlen. Es sei V eine Menge von Unterräumen von L, von denen jeder einen Unterraum des Ranges $r + 1$ enthalte und die überdies die weitere Eigenschaft habe, dass jeder Teilraum von L, dessen Rang $r + 1$ ist, sich als Schnitt von Elementen aus V darstellen lässt. Entsprechend sei V' eine Menge von Unterräumen von L', von denen jeder einen Teilraum des Ranges $s + 1$ enthalte und die weiterhin die Eigenschaft habe, dass jeder Teilraum von L', dessen Rang $s+1$ ist, sich als Schnitt von Elementen aus V' darstellen lässt. Ist dann ρ eine Bijektion von $\mathrm{UR}_r(L) \cup V$ auf $\mathrm{UR}_s(L') \cup V'$, so dass für $X \in \mathrm{UR}_r(L)$ und $Y \in V$ genau dann $X \leq Y$ gilt, wenn $X^\rho \leq Y^\rho$ ist, so gibt es genau einen Isomorphismus τ von L auf L', der ρ induziert.*

Beweis. Setze $U := \mathrm{UR}_r(L)$ und $U' := \mathrm{UR}_s(L')$. Ist $Z \in L$ und gibt es ein $X \in U$ mit $X \leq Z$, so definieren wir Z^σ durch

$$Z^\sigma := \sum_{X \in U,\ X \leq Z} X^\rho.$$

Es ist klar, dass $X^\sigma = X^\rho$ für alle $X \in U$ gilt. Sind Z, $Z' \in L$ und sind Z^σ und Z'^σ definiert, so folgt aus $Z \leq Z'$, dass $Z^\sigma \leq Z'^\sigma$ ist. Ist $Y \in V$, so ist $X^\rho \leq Y^\rho$ für alle $X \in U$, für die $X \leq Y$ gilt. Daher ist $Y^\sigma \leq Y^\rho$.

Es sei $Z \in L$ und der Rang von Z sei $r+1$. Es sei ferner X' ein Unterraum des Ranges s von Z^σ. Auf Grund unserer Annahme über V gibt es ein $Y \in V$ mit $Z \leq Y$. Es gibt weiterhin ein $X \in U$ mit $X^\rho = X'$. Es folgt

$$X^\rho = X^\sigma \leq Z^\sigma \leq Y^\sigma \leq Y^\rho$$

und damit $X \leq Y$. Nach unserer Annahme ist Z Schnitt von Elementen aus V. Somit gilt $X \leq Z$. Dies besagt, dass σ die Menge der Teilräume des Ranges r von Z bijektiv auf die Menge der Teilräume des Ranges s von Z^σ abbildet.

Es sei Z' ein Teilraum des Ranges $s+1$ von Z^σ. Setzt man $M' := \{Y' \mid Y' \in V', Z' \leq Y'\}$, so gilt nach Voraussetzung

$$Z' = \bigcap_{Y' \in M'} Y'.$$

Es gibt nun zwei verschiedene Räume X und Y des Ranges r von L mit $Z' = X^\sigma + Y^\sigma$. Es folgt $Z = X + Y$. Ist nun $A \in V$, so gilt genau dann $X \leq A$, wenn $X^\rho \leq A^\rho$ gilt. Entsprechendes gilt für Y. Setzt man $M := \{A \mid A \in V, Z \leq A\}$, so ist daher $M^\rho = M'$. Ist B ein Teilraum des Ranges r von Z, so gilt $B \leq A$ für alle $A \in M$. Hieraus folgt

$$B^\rho \leq \bigcap_{Y' \in M'} Y' = Z'$$

für alle Teilräume B des Ranges r von Z. Daher ist $Z^\sigma \leq Z'$ und damit $Z^\sigma = Z'$. Somit ist der Rang von Z^σ gleich $s+1$.

Ist nun $r = 1$, so folgt die Behauptung aus 8.1, da man mit Hilfe von ρ^{-1} erschließt, dass in diesem Falle auch $s = 1$ ist. Ist $r > 1$, so folgt die Behauptung mittels des Satzes 8.4, da ρ offensichtlich nicht von einem Antiisomorphismus induziert wird.

Ein typisches Beispiel für die Situation dieses Satzes ist die, dass $r = 1$ und V die Menge der Hyperebenen von L ist. Der Leser formuliere den zu 8.6 dualen Satz.

Es sei L ein projektiver Verband und A sei ein Element von L, welches vom größten Element von L verschieden ist. Mit L_A bezeichnen wir die Menge der $X \in L$ mit $X \not\leq A$. Dann heißt L_A der *vermöge A geschlitzte Raum*. Ist $A = 0$, so ist L_A natürlich im Wesentlichen dasselbe wie L. Ist A eine Hyperebene, so heißt L_A auch *affiner Raum*.

Wir fragen uns nun, wann eine Abbildung σ der Punkte von L_A auf die Punkte von $L'_{A'}$ durch einen Isomorphismus induziert wird. Sicherlich muss σ kollineare Punkte in kollineare Punkte überführen. Diese notwendige Bedingung ist, falls auf jeder Geraden von L mindestens vier Punkte liegen, auch hinreichend. Liegen auf jeder Gerade von L genau drei Punkte und sind L_A und $L'_{A'}$ etwa affine Räume, so erhält jede Bijektion von der Punktmenge von L_A auf die Punktmenge von $L'_{A'}$ die Kollinearität. In diesem Falle muss man noch verlangen, dass auch komplanare Punkte wieder in komplanare Punkte übergehen.

Zwei Elemente X und Y eines projektiven Verbandes heißen *windschief*, falls $X \cap Y = 0$ ist.

8.7. Satz. *Es sei L ein projektiver Verband und G und H seien zwei Geraden von L. Es sei ferner P ein Punkt von $G + H$, der weder auf G noch auf H liege. Genau dann sind G und H windschief, wenn es genau eine Gerade durch P gibt, die sowohl mit G als auch mit H einen Punkt gemeinsam hat.*

Beweis. Wegen $P \leq G + H$ ist

$$\begin{aligned} 4 - \mathrm{Rg}_L(G \cap H) &= \mathrm{Rg}_L(G + H) \\ &= \mathrm{Rg}_L(G + P + H + P) \\ &= \mathrm{Rg}_L(G + P) + \mathrm{Rg}_L(H + P) - \mathrm{Rg}_L\big((G + P) \cap (H + P)\big) \\ &= 6 - \mathrm{Rg}_L\big((G + P) \cap (H + P)\big). \end{aligned}$$

Somit sind G und H genau dann windschief, wenn $(G + P) \cap (H + P)$ eine Gerade ist. Da alle Geraden durch P, die G und H treffen, in $(G+P)\cap(H+P)$ liegen, folgt die Behauptung des Satzes.

8.8. Satz. *Es seien L und L' irreduzible projektive Verbände, die vermöge A bzw. A' geschlitzt seien. Ist σ eine bijektive Abbildung der Menge der Punkte von L_A auf die Menge der Punkte von $L'_{A'}$, die kollineare Punkte auf kollineare Punkte sowie nicht kollineare auf nicht kollineare abbildet, und die im Falle, dass jede Gerade von L genau drei Punkte trägt, noch die weitere Eigenschaft hat, komplanare Punkte auf komplanare Punkte und nicht komplanare Punkte auf ebensolche abzubilden, so gibt es genau einen Isomorphismus τ von L auf L' mit $P^\sigma = P^\tau$ für alle Punkte P von L_A.*

Beweis. Ist $\mathrm{Rg}(L) \leq 2$, so ist die Aussage des Satzes banal. Es sei also $\mathrm{Rg}(L) > 2$.

Da jede Gerade von L, die nicht in A liegt, auf Grund der Irreduzibilität von L mindestens zwei Punkte trägt, die ebenfalls nicht in A liegen, können wir auf Grund der Annahme, dass σ nicht kollineare Punkte auf nicht kollineare Punkte und kollineare Punkte auf kollineare Punkte abbildet, die Abbildung σ fortsetzen auf die Menge der Geraden von L, die nicht in A liegen, indem wir $G^\sigma := P^\sigma + Q^\sigma$ setzen, falls $G = P + Q$ ist.

Es sei nun P ein Punkt auf A und Γ_P sei die Menge der Geraden von L, die durch P gehen, aber nicht in A liegen. Wir setzen $\Gamma'_P := \{G^\sigma \mid G \in \Gamma_P\}$. Wegen $\mathrm{Rg}(L) > 2$ enthält Γ_P und damit Γ'_P mindestens zwei Geraden. Es seien

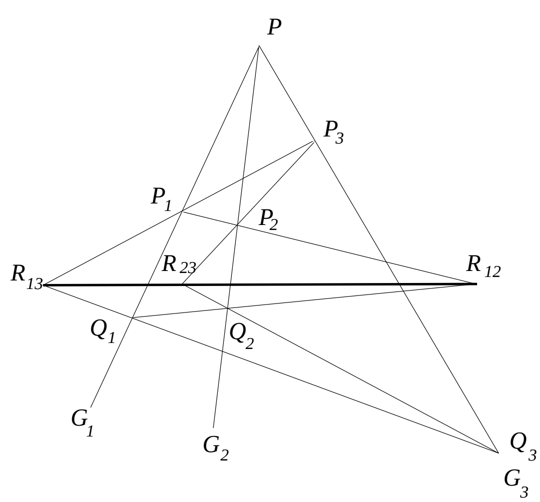
nun G und H zwei verschiedene Geraden aus Γ_P. Dann ist $G + H$ eine Ebene von L. Enthält nun jede Gerade von L genau drei Punkte, so ist auf Grund unserer Annahme $G^\sigma + H^\sigma$ eine Ebene von L'. Enthält jede Gerade von L mehr als drei Punkte, so folgt aus 8.7, dass auch $G^\sigma + H^\sigma$ eine Ebene von L' ist, da es auf Grund der Irreduzibilität von L einen Punkt in $G + H$ gibt, der weder auf G noch auf H liegt. Hieraus folgt, dass $G^\sigma \cap H^\sigma$ ein Punkt ist, der nicht zu $L'_{A'}$ gehört. Somit ist $G^\sigma \cap H^\sigma = A' \cap G^\sigma = A' \cap H^\sigma$. Dies zeigt, dass $G^\sigma \cap A'$ ein Punkt ist, der nicht von der Auswahl von $G \in \Gamma_P$ abhängt.

Ist nun P ein Punkt von L, so setzen wir $P^\tau := P^\sigma$, falls P nicht auf A liegt, und $P^\tau := G^\sigma \cap A'$ mit $G \in \Gamma_P$, falls P auf A liegt. (Hier haben wir vom Auswahlaxiom Gebrauch gemacht.) Es ist nun ein Leichtes zu zeigen, dass τ eine Bijektion der Punkte von L auf die Menge der Punkte von L' ist, die kollineare Punkte auf kollineare Punkte und nicht kollineare Punkte auf nicht kollineare Punkte abbildet. Die Eindeutigkeit von τ ist ebenfalls banal.

9. Der Satz von Desargues

Es sei L ein projektiver Verband. Wir nennen L *desarguessch*, falls in L der folgende *Schließungssatz*, der sog. Satz von Desargues gilt:

Sind G_1, G_2 und G_3 drei verschiedene Geraden, die in einer Ebene von L liegen, ist P ein Punkt mit $P \leq G_i$ für $i := 1, 2, 3$ und sind P_1, P_2, P_3, Q_1, Q_2, Q_3 Punkte mit $P_i \leq G_i$ und $Q_i \leq G_i$ sowie P_i, $Q_i \neq P$ für $i := 1, 2, 3$, ist schließlich für $i \neq j$ auch $P_i + P_j \neq Q_i + Q_j$, so sind die Punkte $R_{ij} := (P_i + P_j) \cap (Q_i + Q_j)$ kollinear.



Satz von Desargues

Es ist zu bemerken, dass die R_{ij} unter den gemachten Voraussetzungen tatsächlich Punkte sind. Man kann den Satz von Desargues grob so formulieren, dass man sagt, dass perspektive Dreiecke stets auch axial sind. Dabei ist P als

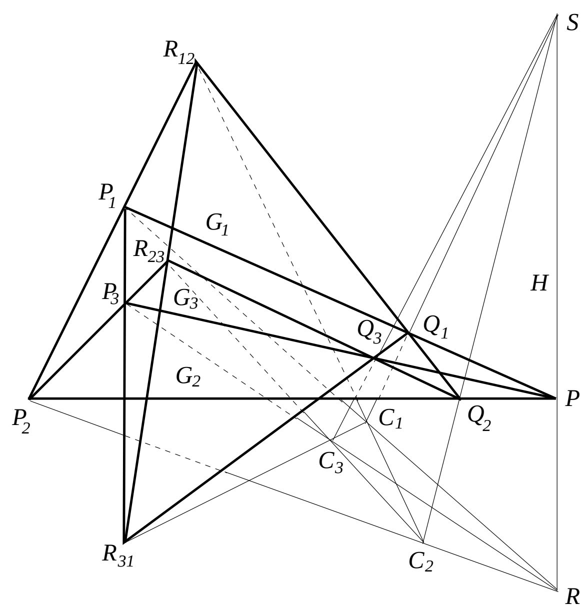
das Perspektivitätszentrum und die Gerade, auf der die Punkte R_{ij} liegen, als die Achse der beiden Dreiecke aufzufassen.

Es erhebt sich die Frage, welche projektiven Räume desarguessch sind. Es ist recht einfach, projektive Ebenen zu konstruieren, die es nicht sind, so dass projektive Geometrien vom Rang 3 nicht immer desarguessch sind. Beispiele hierfür werden wir im letzten Kapitel kennen lernen, die allerdings nicht so einfach zu konstruieren sind, wie gerade behauptet. Für die Theorie der projektiven Ebenen, die uns hier nur am Rande interessiert, sei der Leser auf die Bücher Pickert 1955, Hughes & Piper 1973, Lüneburg 1980 verwiesen.

Für projektive Räume höheren Ranges als 3 gilt jedoch

9.1. Satz. *Ist L ein irreduzibler projektiver Verband und ist* $\mathrm{Rg}(L) \geq 4$*, so ist L desarguessch.*

Beweis. Es seien G_1, G_2 und G_3 drei verschiedene Geraden, die in einer Ebene E von L liegen. Ferner sei P ein Punkt, der mit diesen drei Geraden



Satz von Desargues im Raum

inzidiere. Schließlich seien P_1, P_2, P_3, Q_1, Q_2, Q_3 Punkte mit $P_i, Q_i \leq G_i$ und $P_i, Q_i \neq P$ sowie $P_i + P_j \neq Q_i + Q_j$, falls nur $i \neq j$ ist. Da der Rang von L größer als 3 ist, gibt es eine Gerade H mit $P \leq H$ und $H \not\leq E$. Weil L irreduzibel ist, gibt es zwei verschiedene Punkte R und S auf H, die nicht in E liegen. Die Geraden $P_i + R$ und $Q_i + S$ liegen in der Ebene $G_i + H$. Wegen $R \neq S \neq P \neq R$ und $H \not\leq E$ ist $P_i + R \neq Q_i + S$. Also ist $C_i := (P_i + R) \cap (Q_i + S)$ ein Punkt. Weil die Geraden G_i paarweise verschieden sind, sind auch die Punkte C_i paarweise verschieden.

Gibt es eine Gerade G mit $C_i \leq G$ für alle i, so liegen P_1, P_2 und P_3 in der Ebene $R + G$ und Q_1, Q_2 und Q_3 in der Ebene $S + G$. Hieraus folgt, dass sowohl P_1, P_2, P_3 als auch Q_1, Q_2, Q_3 kollinear sind. In diesem Falle ist $R_{12} = R_{23} = R_{31}$ und daher nichts zu beweisen. Wir dürfen also annehmen, dass $C_1 + C_2 + C_3$ eine Ebene ist. Ist $i \neq j$, so ist $P_i + P_j + R \neq Q_i + Q_j + S$. Da C_i und C_j in beiden Ebenen liegen, ist somit

$$C_i + C_j = (P_i + P_j + R) \cap (Q_i + Q_j + S).$$

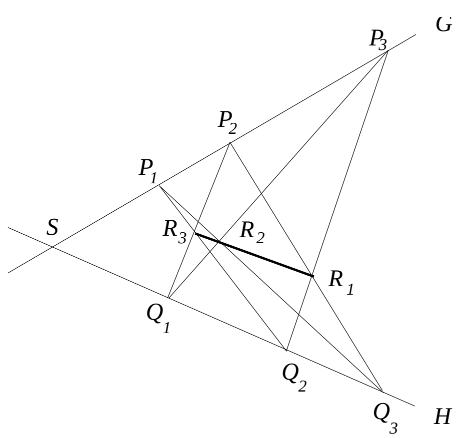
Nun ist R_{ij} ein Punkt, der sowohl in $P_i + P_j + R$ als auch in $Q_i + Q_j + S$ liegt. Also ist $R_{ij} \leq C_i + C_j$ und folglich $R_{ij} \leq E \cap (C_1 + C_2 + C_3)$. Weil die C_i nicht in E liegen, ist $\mathrm{Rg}_L\big(E \cap (C_1 + C_2 + C_3)\big) \leq 2$. Somit sind die R_{ij} kollinear, was zu beweisen war.

Der Satz von Desargues wird im nächsten Kapitel eine entscheidende Rolle bei der Darstellung projektiver Räume mittels Vektorräumen spielen.

10. Der Satz von Pappos

Eine wichtige Rolle spielt auch der Satz von Pappos beim Aufbau der projektiven Geometrie, wenn auch keine so zentrale wie der Satz von Desargues. Er gilt nicht in allen projektiven Räumen. Er ist vielmehr, wie Hilbert als erster bemerkte, gleichbedeutend mit der Kommutativität des der Geometrie zugrunde liegenden Körpers. Hier formulieren wir zunächst den Satz von Pappos und bringen ihn mit gewissen anderen räumlichen Tatsachen in Zusammenhang.

Es seien G und H zwei verschiedene Geraden des projektiven Verbandes L, die sich im Punkte S schneiden. Ferner seien P_1, P_2 und P_3 drei verschiedene Punkte auf G, die auch von S verschieden seien, und Q_1, Q_2 und Q_3 seien drei verschiedene Punkte auf H, die ebenfalls von S verschieden seien. Ist dann $R_3 := (P_1 + P_2) \cap (Q_1 + Q_2)$, $R_1 := (P_2 + P_3) \cap (Q_2 + Q_3)$ und $R_2 := (P_3 + P_1) \cap (Q_3 + Q_1)$, so sind R_1, R_2 und R_3 kollinear.



Satz von Pappos

Wir folgen nun Überlegungen von Dandelin, der die Gültigkeit des Satzes von Pappos aus der Existenz von gewissen räumlichen Konfigurationen erschloss (Germinal Pierre Dandelin, 1794–1847).

Es sei L ein irreduzibler projektiver Verband mit $\mathrm{Rg}(L) \geq 4$. Sind G_1, G_2 und G_3 paarweise windschiefe Geraden von L wie auch H_1, H_2 und H_3 und ist $G_i \cap H_j \neq 0$ für i, $j := 1, 2, 3$, so nennen wir die Konfiguration dieser sechs Geraden *Hexagramme mystique*.

Ist G_1, G_2, G_3, H_1, H_2, H_3 ein Hexagramme mystique, so ist $G_i \neq H_j$. Andernfalls hätte nämlich G_i mit G_k einen Punkt gemein, was jedoch nicht der Fall ist. Setze $S_i := G_i \cap H_i$ für $i := 1, 2, 3$. Dies sind dann Punkte, die überdies nicht kollinear sind. Sie sind ja sicherlich paarweise verschieden, da die G_i windschief sind. Nun ist $S_1 \leq G_1$ und $S_3 \leq H_3$. Wäre $S_2 \leq S_1 + S_3$, so wäre $S_2 \leq G_1 + H_3$. Nun ist $S_2 \not\leq H_3$, da H_2 und H_3 windschief sind. Ferner ist $S_2 \leq G_2$ und $G_2 \cap H_3$ ein Punkt von $G_1 + H_3$, der von S_2 verschieden ist. Also ist

$$G_2 = S_2 + (G_2 \cap H_3) \leq G_1 + H_3.$$

Daraus folgt, da $G_1 + H_3$ ja eine Ebene ist, dass $G_1 \cap G_2 \neq 0$ ist. Dieser Widerspruch zeigt, dass die S_i nicht kollinear sind.

Nach diesen Vorbemerkungen sind wir nun in der Lage, den Satz von Dandelin zu beweisen.

10.1. Satz von Dandelin. *Es seien G und H zwei verschiedene Geraden eines irreduziblen projektiven Verbandes L, dessen Rang mindestens 4 sei. Ferner sei $S := G \cap H$ ein Punkt. Weiter seien P_1, P_2 und P_3 drei verschiedene Punkte auf G und Q_1, Q_2 und Q_3 drei verschiedene Punkte auf H und alle diese Punkte seien von S verschieden. Setze*

$$\begin{aligned} R_3 &:= (P_1 + Q_2) \cap (P_2 + Q_1) \\ R_1 &:= (P_2 + Q_3) \cap (P_3 + Q_2) \\ R_2 &:= (P_3 + Q_1) \cap (P_1 + Q_3). \end{aligned}$$

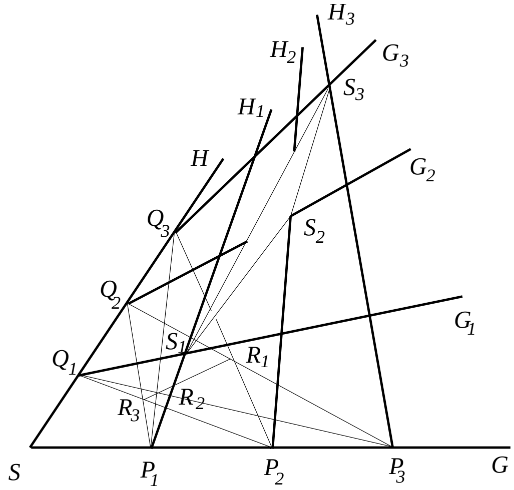
Die Punkte R_1, R_2 und R_3 sind sicher dann kollinear, wenn es ein Hexagramme mystique G_1, G_2, G_3, H_1, H_2, H_3 gibt mit $P_i \leq H_i$, $Q_i \leq G_i$ und G_i, $H_i \leq G + H$ für $i := 1, 2, 3$.

Beweis. Setze $E_{ij} := G_i + H_j$. Dann ist E_{ij}, da G_i und H_j verschiedene Geraden sind, die sich in einem Punkte schneiden, eine Ebene. Setze ferner $S_i := G_i \cap H_i$. Nun ist

$$R_3 \leq P_1 + Q_2 \leq H_1 + G_2 = E_{21}$$

und

$$R_3 \leq P_2 + Q_1 \leq H_2 + G_1 = E_{12}.$$



Satz von Dandelin

Ferner folgt $E_{12} \neq E_{21}$, da G_1 und G_2 ja windschief sind. Außerdem ist $S_1 \leq H_1 \leq E_{21}$ und $S_2 \leq G_2 \leq E_{21}$. Ebenso folgt, dass $S_1, S_2 \leq E_{12}$ ist. Weil die S_i nach unserer Vorbemerkung nicht kollinear sind, ist also

$$S_1 + S_2 = E_{12} \cap E_{21}.$$

Hieraus folgt

$$R_3 \leq E_{12} \cap E_{21} = S_1 + S_2 \leq S_1 + S_2 + S_3.$$

Entsprechend folgt, dass auch R_1 und R_2 in $S_1 + S_2 + S_3$ liegen. Wären die R_i nicht kollinear, so wäre

$$G + H = R_1 + R_2 + R_3 = S_1 + S_2 + S_3.$$

Da die S_i nicht kollinear sind, liegt wenigstens einer von ihnen nicht auf H. Es sei etwa $S_i \leq H$. Dann ist $S_i \neq Q_i$ und daher $G_i = S_i + Q_i \leq G + H$ im Widerspruch zu unserer Voraussetzung. Dieser Widerspruch zeigt, dass die R_i doch kollinear sind.

Der Satz von Dandelin gestattet auch eine Umkehrung, die wir nun formulieren werden. Dieser Satz ist mit den noch zu entwickelnden analytischen Methoden leicht zu beweisen. Ein Beweis an dieser Stelle ist möglich, aber knifflig. Der Leser ist herausgefordert, seine Kräfte zu erproben.

Es seien G_1, G_2 und G_3 drei paarweise windschiefe Geraden eines irreduziblen projektiven Verbandes. Ist H eine Gerade und gilt $H \cap G_i \neq 0$ für alle i, so heißt H eine *Transversale* von G_1, G_2, G_3. Eine solche gibt es nur dann, wenn der von den G_i aufgespannte Teilraum den Rang 4 hat. In diesem Falle gibt es aber sehr viele Transversalen, nämlich durch jeden Punkt von G_i genau eine (Satz 8.7).

10.2. Satz. *Es sei L ein irreduzibler projektiver Verband mit* $\mathrm{Rg}(L) \geq 4$. *Genau dann gilt in L der Satz von Pappos, wenn für jedes Hexagramme mystique G_1, G_2, G_3, H_1, H_2, H_3 gilt: ist H eine Transversale der G_i und G eine Transversale der H_j, so ist $G \cap H \neq 0$.*

Beweis. Nicht triviale Übungsaufgabe.

Wir beenden das lange erste Kapitel mit einer Übungsaufgabe, die man mit Hilfe des Satzes von Pappos in jeder papposschen Ebene lösen kann, deren Geraden je mindestens vier Punkte tragen (Jackson 1821).

Your aid I want
nine trees to plant
in rows just half a score.
And let there be
in each row three.
Solve this, I ask no more.

II.

Die Struktursätze

In diesem Kapitel geht es nun darum, die Struktursätze der projektiven Geometrie zu etablieren. Es sind drei Sätze. Der erste besagt, dass ein desarguesscher, irreduzibler projektiver Verband nichts Anderes ist als der Unterraumverband eines geeigneten Vektorraumes. Der zweite besagt, dass Isomorphismen zwischen solchen Verbänden durch semilineare Abbildungen induziert werden, während der letzte besagt, dass eine Korrelation eines solchen Verbandes stets durch eine Semibilinearform dargestellt wird. Mit diesen Sätzen hat man dann das Instrumentarium der linearen Algebra an der Hand, wenn man tiefer in die Theorie der projektiven Geometrien eindringen will.

1. Zentralkollineationen

Im Folgenden betrachten wir nur irreduzible projektive Verbände. Es sei L ein solcher mit $\mathrm{Rg}(L) \geq 3$. Wir bezeichnen wieder, wie bisher, mit Π das größte und mit 0 das kleinste Element von L. Ist σ eine Kollineation von L und gibt es eine Hyperebene H von L mit der Eigenschaft

(A) Ist $X \leq H$, so ist $X^\sigma = X$,

so nennen wir σ *axiale Kollineation* und H *Achse* von σ. Da nach I.2.11 jedes Element von L die obere Grenze der in ihm liegenden Punkte ist, ist (A) gleichbedeutend mit

(A*) Ist P ein Punkt auf H, so ist $P^\sigma = P$,

Ist σ eine Kollineation von L und gibt es einen Punkt P in L mit der Eigenschaft

(Z) Ist $P \leq X$, so ist $X^\sigma = X$,

so nennen wir σ *zentral* und P heißt *Zentrum* von σ. Da $P \leq P$ ist, ist $P^\sigma = P$. Daher induziert σ eine Kollineation in Π/P, die gleich der Identität ist. Weil Π/P ein projektiver Verband ist, ist (Z) gleichbedeutend mit

(Z*) Ist G eine Gerade durch P, so ist $G^\sigma = G$.

Es gilt nun der folgende Satz.

1.1. Satz. *Ist L ein irreduzibler projektiver Verband, dessen Rang mindestens 3 ist, und ist σ eine Kollineation von L, so gilt:*
a) *Ist σ axial und hat σ zwei verschiedene Achsen, oder*
b) *ist σ zentral und hat σ zwei verschiedene Zentren,*
so ist $\sigma = 1_L$.

Beweis. a) Es seien H und K zwei verschiedene Achsen von σ. Ferner sei P ein Punkt von L. Liegt P auf H oder K, so ist $P^\sigma = P$. Es liege P weder auf H noch auf K. Da $\mathrm{Rg}(L) \geq 3$ ist, ist $\mathrm{Rg}_L(H) \geq 2$. Es gibt folglich eine Gerade G mit $G \leq H$ und $G \not\leq H \cap K$. Wegen $\mathrm{KoRg}_H(H \cap K) = 1$ ist $G \cap H \cap K$ ein Punkt. Weil L irreduzibel ist, gibt es folglich zwei Punkte R und S auf G, die nicht in $H \cap K$ liegen. Nun ist $R + S = G \cap H$. Hiermit folgt, dass $R + P \neq S + P$, und weiter, dass

$$(R + P) \cap (S + P) = P$$

ist. Ferner sind $U := K \cap (R+P)$ und $V := K \cap (S+P)$ Punkte, die von R und S verschieden sind, da weder R noch S in K liegt. Daher ist $R + P = R + U$ und $S + P = S + V$. Es folgt, dass

$$P = (R + U) \cap (S + V)$$

ist. Damit erhalten wir schließlich

$$\begin{aligned} P^\sigma &= \big((R + U) \cap (S + V)\big)^\sigma = (R^\sigma + U^\sigma) \cap (s^\sigma + V^\sigma) \\ &= (R + U) \cap (S + V) = P. \end{aligned}$$

Damit ist gezeigt, dass σ alle Punkte von L festlässt, woraus folgt, dass $\sigma = 1_L$ ist.

b) Da der zu einem projektiven Verband duale Verband nur dann wieder ein projektiver Verband ist, wenn der Rang des gegebenen Verbandes endlich ist — wir reden hier von irreduziblen projektiven Verbänden —, können wir uns zum Beweise von b) nicht auf die Aussage a) berufen, wir müssen sie vielmehr getrennt beweisen.

Es seien P und Q zwei verschiedene Zentren von σ. Ferner sei X ein Punkt, der nicht auf $P + Q$ liegt. Dann sind $P + X$ und $Q + X$ zwei verschiedene Geraden, so dass $X = (P + X) \cap (Q + X)$ gilt. Weil die Geraden durch P wie auch die Geraden durch Q festbleiben, folgt $X^\sigma = X$. Somit lässt σ alle Punkte von L_{P+Q} fest. Mittels I.8.8 folgt schließlich, dass $\sigma = 1_L$ ist.

Damit ist alles bewiesen.

1.2. Satz. *Es sei L ein irreduzibler projektiver Verband mit $\mathrm{Rg}(L) \geq 3$ und σ sei eine Kollineation von L. Genau dann ist σ axial, wenn σ zentral ist.*

Beweis. Es sei σ axial und H sei eine Achse von σ. Ist P ein Punkt von L mit $P^\sigma = P \not\leq H$ und ist G eine Gerade durch P, so ist $G = P + (G \cap H)$. Hieraus folgt

$$G^\sigma = \big(P + (G \cap H)\big)^\sigma = P^\sigma + (G \cap H)^\sigma = P + (G \cap H) = G,$$

so dass P wegen (Z*) ein Zentrum von σ ist.

Es sei nun $P \neq P^\sigma$ für alle Punkte P, die nicht auf H liegen. Es sei P ein solcher Punkt. Dann ist $P + P^\sigma$ eine Gerade. Ferner gilt $\Pi = P + H = P^\sigma + H$.

Hieraus folgt mit Hilfe des Modulargesetzes

$$\begin{aligned} P + P^\sigma &= (P + P^\sigma) \cap (P^\sigma + H) = P^\sigma + \big((P + P^\sigma) \cap H\big) \\ &= P^\sigma + \big((P + P^\sigma) \cap H\big)^\sigma = \big(P + ((P + P^\sigma) \cap H)\big)^\sigma \\ &= \big((P + P^\sigma) \cap (P + H)\big)^\sigma = (P + P^\sigma)^\sigma, \end{aligned}$$

so dass $P + P^\sigma$ eine Fixgerade von σ ist.

Es sei F ein Punkt mit $F \not\leq H$. Dann ist also $F + F^\sigma$ eine Fixgerade von σ. Setze $C := (F + F^\sigma) \cap H$. Dann ist C ein Punkt. Wir zeigen, dass C Zentrum von σ ist. Es sei G eine Gerade durch C. Ist $G \leq H$ oder $G = F + F^\sigma$, so ist G eine Fixgerade von σ. Es sei also $G \not\leq H$ und $G \neq F + F^\sigma$. Es gibt dann einen Punkt P auf G, der nicht auf $F + F^\sigma$ liegt. Wegen

$$(F + F^\sigma) \cap G = C = G \cap H$$

ist $P \not\leq H$ und daher $P \neq P^\sigma$. Setze $R := (P + F) \cap H$. Dann ist R ein Punkt, da ja $P \neq F$ ist. Es folgt $P + F = P + R = F + R$. Wegen $R^\sigma = R$ ist daher

$$\begin{aligned} P + P^\sigma + F + F^\sigma &= P^\sigma + P + F + F^\sigma = P^\sigma + P + R + F^\sigma \\ &= P^\sigma + P + R^\sigma + F^\sigma = P^\sigma + P + (R + F)^\sigma \\ &= P^\sigma + P + (P + F)^\sigma = P^\sigma + P + F^\sigma. \end{aligned}$$

Wegen $P \not\leq F + F^\sigma$ ist also

$$3 \leq \mathrm{Rg}_L(P + P^\sigma + F + F^\sigma) = \mathrm{Rg}_L(P^\sigma + P + F^\sigma) \leq 3.$$

Hieraus folgt, dass $(P + P^\sigma) \cap (F + F^\sigma)$ ein Punkt ist. Weil $P + P^\sigma$ und $F + F^\sigma$ Fixgeraden von σ sind, ist dieser Punkt ein Fixpunkt von σ, liegt also auf H. Daher ist $(P + P^\sigma) \cap (F + F^\sigma) = C$. Hieraus folgt weiter, dass $P + P^\sigma = P + C = G$ ist. Somit ist $G^\sigma = G$, so dass C in der Tat ein Zentrum von σ ist.

Es sei nun σ zentral und P sei ein Zentrum von σ. Ist H eine Hyperebene, die nicht durch P geht und die unter σ festbleibt, so ist H eine Achse von σ, wie unschwer zu sehen ist. Es gelte also $H^\sigma \neq H$ für alle nicht durch P gehenden Hyperebenen H. Es sei H eine solche Hyperebene. Dann ist $P \not\leq H \cap H^\sigma$, so dass $A := P + (H \cap H^\sigma)$ eine Hyperebene ist. Weil $P \leq A$ ist, ist $A^\sigma = A$. Nun ist

$$A \cap H = \big(P + (H \cap H^\sigma)\big) \cap H = (P \cap H) + (H \cap H^\sigma) = H \cap H^\sigma.$$

Ebenso folgt, dass $A \cap H^\sigma = H \cap H^\sigma$ ist. Also ist $A \cap H = A \cap H^\sigma$ und daher

$$(A \cap H)^\sigma = A^\sigma \cap H^\sigma = A \cap H^\sigma = A \cap H.$$

Insbesondere folgt, dass $(H \cap H^\sigma)^\sigma = H \cap H^\sigma$ ist.

Es sei nun K ein Komplement von P. Dann ist $(K \cap K^\sigma)^\sigma = K \cap K^\sigma$. Weil alle Geraden durch P unter σ festbleiben, lässt σ alle Punkte von $K \cap K^\sigma$ fest.

Somit ist $K \cap K^\sigma \leq A$ und daher $A \cap K = K \cap K^\sigma$. Ist nun X ein von P verschiedener Punkt von A, so gibt es nach I.1.8 ein Komplement K von P, welches X enthält. Es folgt $X \leq A \cap K = K \cap K^\sigma$, so dass X ein Fixpunkt von σ ist. Damit ist A als Achse von σ erkannt und der Satz in allen seinen Teilen bewiesen.

Die zentralen bzw. axialen Kollineationen eines projektiven Verbandes werden wir im folgenden auch *Perspektivitäten* nennen. Nach dem gerade bewiesenen Satz besteht zwischen ihnen ja kein Unterschied. Ist σ eine Perspektivität mit dem Zentrum P und der Achse H und ist $P \leq H$, so nennen wir σ *Elation*. Ist $P \not\leq H$, so nennen wir σ *Streckung* oder *Homologie*. Ist H eine Hyperebene, so bezeichne $\Delta(H)$ die Menge aller Perspektivitäten mit der Achse H. Offensichtlich ist $\Delta(H)$ eine Untergruppe der Gruppe aller Kollineationen von L. Entsprechend bezeichnen wir für einen Punkt P mit $\Delta(P)$ die Menge aller Perspektivitäten mit dem Zentrum P. Auch dies ist eine Untergruppe der Gruppe aller Kollineationen von L. Schließlich setzen wir $\Delta(P,H) := \Delta(P) \cap \Delta(H)$. Diese Gruppen werden wir nun eingehender untersuchen.

1.3. Satz. *Ist P ein Punkt und H eine Hyperebene des irreduziblen projektiven Verbandes L, ist ferner $1 \neq \sigma \in \Delta(P,H)$ und ist X ein Element von L mit $X^\sigma = X$, so ist $P \leq X$ oder $X \leq H$.*

Beweis. Es sei $P \not\leq X$. Ist dann Q ein Punkt von X, so ist Q Fixpunkt von σ, da ja $Q = (P+Q) \cap X$ ist. Wäre nun $X \not\leq H$, so gäbe es insbesondere einen Punkt Q auf X, der nicht in H läge. Dieser Punkt wäre dann aber ein zweites Zentrum von σ, da ja jede Gerade durch Q die Hyperebene H in einem Punkte träfe und somit unter σ fix bliebe. Diese widerspräche aber 1.1b).

1.4. Satz. *Es seien σ und τ zwei Elationen des irreduziblen projektiven Verbandes L. Haben σ und τ die gleiche Achse aber verschiedene Zentren oder das gleiche Zentrum aber verschiedene Achsen, so ist $\sigma\tau = \tau\sigma$.*

Beweis. Es sei H Achse von σ und τ. Ferner sei P ein Zentrum von σ und Q ein solches von τ und es sei $P \neq Q$. Es ist $\tau^{-1}\sigma\tau$ eine Elation mit dem Zentrum P^τ und der Achse H^τ. Wegen $P \leq H$ und $\tau \in \Delta(Q,H)$ bleiben P und H unter τ fest. Also gilt $\sigma^{-1}, \tau^{-1}\sigma\tau \in \Delta(P,H)$ und damit $\sigma^{-1}\tau^{-1}\sigma\tau \in \Delta(P,H)$.

Fängt man mit $\sigma^{-1}\tau^{-1}\sigma$ an, so sieht man ganz entsprechend, dass auch $\sigma^{-1}\tau^{-1}\sigma\tau \in \Delta(Q,H)$ gilt. Mit Satz 1.1 folgt daher

$$\sigma^{-1}\tau^{-1}\sigma\tau \in \Delta(P,H) \cap \Delta(Q,H) = \{1\}.$$

Also ist $\sigma\tau = \tau\sigma$.

Die zweite Aussage von 1.4 beweist sich analog.

Mit $\mathrm{E}(H)$ bezeichnen wir im folgenden die Menge aller Elationen mit der Achse H und mit $\mathrm{E}(P)$ die Menge aller Elationen mit dem Zentrum P. Ferner setzen wir $\mathrm{E}(P,H) := \mathrm{E}(P) \cap \mathrm{E}(H)$. Dies ist natürlich nur dann von Interesse, wenn $P \leq H$ ist.

1.5. Satz. *Ist L ein irreduzibler projektiver Verband, ist H eine Hyperebene und P ein Punkt von L, so sind $\mathrm{E}(H)$ und $\mathrm{E}(P)$ Untergruppen der Kollineationsgruppe von L.*

Beweis. Es seien σ, $\tau \in \mathrm{E}(H)$. Haben σ und τ das gleiche Zentrum, so hat auch $\sigma\tau$ dieses Zentrum, so dass das Produkt in $\mathrm{E}(H)$ liegt. Wir nehmen nun an, dass σ das Zentrum P und τ das Zentrum Q habe und dass $P \neq Q$ sei. Wir dürfen weiter annehmen, dass σ und τ beide von der Identität verschieden sind. Dann ist $\sigma\tau \neq 1$. Es sei R das eindeutig bestimmte Zentrum der Perspektivität $\sigma\tau$. Dann ist R^σ das Zentrum von $\sigma^{-1}\sigma\tau\sigma = \tau\sigma$. Nach 1.4 ist $\tau\sigma = \sigma\tau$, so dass also $R^\sigma = R$ ist. Nach 1.3 ist daher $R = P$ oder $R \leq H$. Wegen $P \leq H$ gilt in jedem Falle $R \leq H$. Somit ist $\sigma\tau \in \mathrm{E}(H)$. Schließlich ist klar, dass mit σ auch σ^{-1} zu $\mathrm{E}(H)$ gehört.

Ebenso zeigt man, dass auch $\mathrm{E}(P)$ eine Gruppe ist.

Wir stellen nun die Frage nach der Existenz von Perspektivitäten und wir werden sehen, dass uns mit dem Satz von Desargues ein Mittel in die Hand gegeben ist, solche zu konstruieren. Ist L ein irreduzibler projektiver Verband und ist $\mathrm{Rg}(L) \geq 4$, so gilt nach I.9.1 in L der Satz von Desargues. Ist $\mathrm{Rg}(L) = 3$, so müssen wir seine Gültigkeit voraussetzen. Wir beweisen zunächst.

1.6. Satz. *Ist L ein desarguesscher, irreduzibler projektiver Verband, ist H eine Hyperebene von L und sind P, A und B drei verschiedene, kollineare Punkte von L mit A, $B \not\leq H$, so gibt es genau ein $\sigma \in \Delta(P, H)$ mit $A^\sigma = B$.*

Beweis. Aus 1.3 folgt, dass es höchstens ein solches σ gibt. Ist nämlich τ ein weiteres Element aus $\Delta(P, H)$ mit $A^\tau = B$, so ist $\sigma\tau^{-1} \in \Delta(P, H)$. Andererseits ist A ein von P verschiedener Fixpunkt von $\sigma\tau^{-1}$, der auch nicht in H liegt. Also ist $\sigma\tau^{-1} = 1$, so dass $\sigma = \tau$ ist.

Wir zeigen nun die Existenz eines solchen σ. Dies ist sehr einfach, falls auf jeder Geraden von L genau drei Punkte liegen. Wegen $P \leq A + B$ und A, $B \not\leq H$ ist dann $P \leq H$. Wir definieren σ durch $X^\sigma = X$, falls X ein Punkt von H ist. Ist X ein Punkt des geschlitzten Raumes L_H, so sei X^σ der von X und P verschiedene dritte Punkt auf $X + P$. Offenbar ist $\sigma^2 = 1$, so dass σ eine Bijektion der Punktmenge von L auf sich ist. Um zu zeigen, dass σ eine Kollineation ist, genügt es wegen $\sigma^2 = 1$ zu zeigen, dass σ kollineare Punkte auf kollineare Punkte abbildet. Dies ist aber, da auf jeder Geraden von L nur drei Punkte liegen, eine unmittelbare Konsequenz des Veblen-Young Axioms. Wir dürfen im Folgenden also annehmen, dass auf jeder Geraden von L mindestens vier Punkte liegen.

Wir betrachten den geschlitzten Raum L_{A+B}. Es sei X ein Punkt dieses Raumes. Ist X ein Punkt von H, so setzen wir $X^\sigma := X$ und $X^\tau := X$. — Wir definieren neben σ also auch gleichzeitig die zu σ inverse Abbildung τ. — Liegt X nicht in H, so setzen wir

$$X^\sigma := \big(((X + A) \cap H) + B\big) \cap (P + X)$$

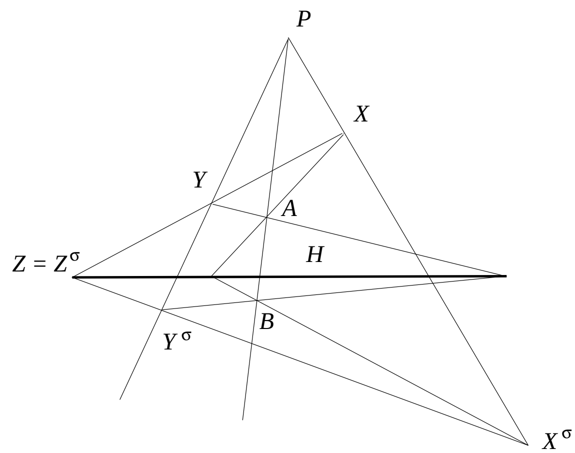
bzw.

$$X^\tau := \big(((X + B) \cap H) + A\big) \cap (P + X).$$

Offensichtlich ist $\sigma\tau = 1 = \tau\sigma$, so dass σ und τ zueinander inverse Bijektionen der Punktmenge von L_{A+B} auf sich sind. Es genügt nun im Folgenden zu zeigen,

dass σ kollineare Punkte auf kollineare Punkte abbildet, da τ als Abbildung des gleichen Typs dann ebenfalls diese Eigenschaft hat.

Es seien nun X, Y und Z drei kollineare Punkte von L_{A+B}. Wir dürfen oBdA annehmen, dass $Z \leq H$ und $X, Y \not\leq H$ gilt. Ist $P \leq X+Y$ oder $A \leq X+Y$, so folgt unmittelbar aus der Definition von σ, dass X^σ, Y^σ und $Z^\sigma = Z$ kollinear sind. Es sei also P, $A \not\leq X+Y$. Dann ist auch P, $B \not\leq X^\sigma + Y^\sigma$. Die Dreiecke



A, X, Y und B, X^σ, Y^σ erfüllen daher die Voraussetzungen des Satzes von Desargues. Somit sind die Punkte

$$(A+Y) \cap (B+Y^\sigma),$$
$$(A+X) \cap (B+X^\sigma),$$
$$(X+Y) \cap (X^\sigma+Y^\sigma)$$

kollinear. Da die ersten beiden Punkte in H liegen, liegt auch der dritte Punkt in H. Folglich ist

$$(X+Y) \cap (X^\sigma + Y^\sigma) = (X+Y) \cap H = Z,$$

so dass die Punkte X^σ, Y^σ und $Z = Z^\sigma$ kollinear sind. Damit ist gezeigt, dass σ kollineare Punkte auf kollineare Punkte abbildet. Nach unserer Vorbemerkung bildet σ dann auch nicht kollineare Punkte auf nicht kollineare Punkte ab. Weil auf jeder Geraden von L mindestens vier Punkte liegen, ist daher Satz I.8.8 anwendbar, so dass σ durch eine Kollineation von L induziert wird. Diese gehört offensichtlich zu $\Delta(P, H)$ und bildet A auf B ab. Damit ist alles bewiesen.

Projektive Ebenen sind nicht immer desarguessch. Es ist daher angebracht, die Situation in diesem Falle etwas genauer zu analysieren. Die nun folgende Analyse stammt von R. Baer (Baer 1942).

Es sei L eine projektive Ebene, dh. ein irreduzibler projektiver Verband des Ranges 3. Ferner sei P ein Punkt und G eine Gerade von L. Wir sagen, dass in L der (P, G)-*Satz von Desargues* erfüllt sei, wenn Folgendes gilt:

Sind G_1, G_2, G_3 drei verschiedene Geraden von L, die durch P gehen, und sind P_i, Q_i für $i := 1, 2, 3$ Punkte auf G_i, die von P verschieden sind und auch nicht auf G liegen, ist $P_i + P_j \neq Q_i + Q_j$ für $i \neq j$ und liegen die Punkte

$$R_{12} := (P_1 + P_2) \cap (Q_1 + Q_2)$$

und

$$R_{13} := (P_1 + P_3) \cap (Q_1 + Q_3)$$

auf G, so liegt auch der Punkt

$$R_{23} := (P_2 + P_3) \cap (Q_2 + Q_3)$$

auf G.

Ferner sagen wir, dass L eine (P, G)-*transitive* Ebene ist, wenn es zu jedem Punktepaar A, B mit $P \neq A \not\leq G$ und $P \neq B \not\leq G$ sowie $P + A = P + B$ ein $\sigma \in \Delta(P, G)$ mit $A^\sigma = B$ gibt. Der Beweis von 1.6 liefert auch die Gültigkeit einer Schlussrichtung in

1.7. Satz. *Eine projektive Ebene ist genau dann (P, G)-transitiv, wenn in ihr der (P, G)-Satz von Desargues gilt.*

Dies ist wieder eine gute Gelegenheit für den Leser, seine bereits erworbenen Fähigkeiten zu erproben und zu zeigen, dass aus der (P, G)-Transitivität der (P, G)-Satz von Desargues folgt. Dazu wähle er sich ein $\sigma \in \Delta(P, G)$ mit $P_1^\sigma = Q_1$ und verfolge die Wirkung von σ auf den Rest der Figur.

1.8. Korollar. *Eine projektive Ebene ist genau dann desarguessch, wenn sie (P, G)-transitiv ist für alle Punkt-Geradenpaare (P, G).*

Weiter gilt

1.9. Korollar. *Ist L eine desarguessche projektive Ebene, so ist auch L^d desarguessch.*

Dies folgt aus 1.8 und der Bemerkung, dass L offensichtlich genau dann (P, G)-transitiv ist, wenn L^d eine (G, P)-transitive Ebene ist.

Ein Element g einer Gruppe G heißt *Involution*, wenn $g^2 = 1 \neq g$ ist.

1.10. Satz. *Es sei L ein irreduzibler projektiver Verband, dessen Rang mindestens 3 sei. Ferner seien P und Q zwei verschiedene Punkte und H eine Hyperebene von L mit $P, Q \not\leq H$. Ist dann ρ eine Involution aus $\Delta(P, H)$ und σ eine Involution aus $\Delta(Q, H)$, so ist $1 \neq \rho\sigma \in \mathrm{E}((P + Q) \cap H, H)$.*

Beweis. Natürlich gilt $\rho\sigma \in \Delta(H)$. Ferner gilt $(P + Q)^{\rho\sigma} = P + Q$. Wegen $P + Q \not\leq H$ liegt das Zentrum R von $\rho\sigma$ nach 1.3 auf $P + Q$, da ja offenbar $\rho\sigma \neq 1$ ist. Es bleibt zu zeigen, dass R auf H liegt.

Wegen $R^{\rho\sigma} = R$ und $\sigma^2 = 1$ ist $R^\rho = R^{\rho\sigma^2} = R^\sigma$. Hieraus folgt

$$(R^\rho)^{\rho\sigma} = R^{\rho^2\sigma} = R^\sigma = R^\rho.$$

Nach 1.3 gilt daher $R^\rho = R$ oder $R^\rho \leq H$. Im letzteren Falle folgt $R^\rho = R^{\rho^2} = R$ und damit $R \leq H$. Im ersten Fall folgt wieder mit 1.3, dass $R \leq H$ oder $R = P$

ist. Wäre $R = P$ so folgte $P = R = R^{\rho\sigma} = P^{\sigma}$ und mit $P \not\leq H$ weiter der Widerspruch $P = Q$. Also ist in jedem Falle $R \leq H$.

Der nächste Satz ist vor allem für projektive Ebenen interessant, da eine ebene projektive Geometrie nicht notwendig desarguessch ist.

1.11. Satz. *Es sei L ein irreduzibler projektiver Verband mit* $\mathrm{Rg}(L) \geq 3$ *und jede Gerade von L trage wenigstens vier Punkte. Ferner sei H eine Hyperebene und P und Q seien zwei verschiedene Punkte von L, die nicht auf H liegen. Ist* $\mathrm{Rg}(L) = 3$, *so werde noch vorausgesetzt, dass L sowohl (P, H)- als auch (Q, H)-transitiv sei. Dann ist $\Delta(X, H)$ für alle Punkte X auf $P + Q$ eine Untergruppe der von $\Delta(P, H)$ und $\Delta(Q, H)$ erzeugten Gruppe. Ist* $\mathrm{Rg}(L) = 3$, *so ist L für alle diese Punkte (X, H)-transitiv.*

Beweis. Es sei G die von $\Delta(P, H)$ und $\Delta(Q, H)$ erzeugte Gruppe.

j) Die Gruppe G operiert scharf zweifach transitiv auf der Menge Ω der von $(P + Q) \cap H$ verschiedenen Punkte auf $P + Q$.

Nach 1.6 bzw. auf Grund unserer Annahme operiert $\Delta(P, H)$ auf $\Omega - \{P\}$ transitiv. Weil $\Omega - \{P\}$ auf Grund der Annahme, dass jede Gerade mindestens vier Punkte trägt, wenigstens zwei Punkte enthält, enthält $\Delta(Q, H)$ wenigstens ein von 1 verschiedenes Element, so dass P auf Grund von 1.6 bzw. unserer Annahme über $\Delta(Q, H)$ und wegen 1.1 kein Fixpunkt von $\Delta(Q, H)$ ist. Daher ist G auf Ω zweifach transitiv. Weil G nur aus axialen Kollineationen mit der Achse H besteht, folgt mit 1.1, dass das einzige Element in G, welches zwei Fixpunkte außerhalb H hat, die Identität ist. Folglich ist G scharf zweifach transitiv auf Ω.

ij) Es ist $\mathrm{E}((P + Q) \cap H, H) \cap G \neq \{1\}$.

Es seien A und B zwei verschiedene Punkte aus Ω. Nach j) gibt es ein $\gamma \in G$ mit $A^{\gamma} = B$ und $B^{\gamma} = A$. Es folgt $A^{\gamma^2} = A$ und $B^{\gamma^2} = B$. Nach 1.1 ist daher $\gamma^2 = 1$. Wegen $A \neq B$ ist γ daher eine Involution. Ist $\gamma \in \mathrm{E}((P+Q) \cap H, H)$, so sind wir fertig. Es sei also $\gamma \notin \mathrm{E}((P+Q) \cap H, H)$. Dann liegt das Zentrum von γ in Ω. Weil dieses Zentrum auf Grund von j) kein Fixelement von G ist, gibt es noch eine zweite involutorische Streckung in G, deren Zentrum vom Zentrum von γ verschieden ist. Mit 1.10 folgt daher die Behauptung.

iij) Es ist $\mathrm{E}((P + Q) \cap H, H) \subseteq G$ und $\mathrm{E}((P + Q) \cap H, H)$ operiert transitiv auf Ω.

Die Gruppe $\mathrm{E}((P+Q) \cap H, H) \cap G$ ist nach ij) ein nicht trivialer Normalteiler von G. Weil G nach j) zweifach transitiv operiert, operiert dieser Normalteiler auf Ω transitiv. Mit 1.1 folgt hieraus, dass $\mathrm{E}((P + Q) \cap H, H) \cap G = \mathrm{E}((P + Q) \cap H, H)$ ist.

Dass schließlich auch alle $\Delta(X, H)$ für $X \in \Omega$ in G enthalten sind und auf $\Omega - \{X\}$ transitiv operieren, folgt aus der Transitivität von G auf Ω. Damit ist alles bewiesen.

Soviel an Bemerkungen zu der Situation im ebenen Fall. Wir wenden uns nun wieder der allgemeinen Situation zu.

1.12. Satz. *Es sei H eine Hyperebene des irreduziblen projektiven Verbandes L. Sind σ, $\tau \in \Delta(H)$ und ist σ, τ, $\sigma\tau \neq 1$, ist ferner P das Zentrum von σ, ist Q das Zentrum von τ und R das von $\sigma\tau$, so ist $R \leq P + Q$.*

Beweis. Ist $P = Q$, so ist $R = P = Q \leq P + Q$. Es sei also $P \neq Q$. Setze $G := P + Q$. Dann ist $G^\sigma = G = G^\tau$. Ist $G \not\leq H$, so folgt aus 1.3, dass $R \leq G$ ist. Es sei also $G \leq H$. Weil σ und τ Elationen sind, ist auch $\sigma\tau$ nach 1.5 eine solche. Folglich ist $R \leq H$. Es gibt eine Ebene E — evtl. das größte Element von L — mit $G = E \cap H$. Weil E unter σ und τ festbleibt, bleibt sie auch unter $\sigma\tau$ fest. Wegen $E \not\leq H$ folgt mit 1.3, dass $R \leq E$ ist. Also ist $R \leq E \cap H = G$.

Es sei L ein irreduzibler projektiver Verband, dessen Rang mindestens gleich 3 sei. Ferner sei H eine Hyperebene von L. Ist $0 \neq X \in L$, so bezeichnen wir mit $\Delta(X, H)$ die Menge der Perspektivitäten, deren Zentrum in X liegen. Mit 1.12 folgt dann, dass $\Delta(X)$ eine Untergruppe von $\Delta(H)$ ist. Wir setzen noch $\Delta(0, H) := \{1\}$. Es ist $\Delta(\Pi, H) = \Delta(H)$ und $\Delta(H, H) = \mathrm{E}(H)$. Ist $X \leq H$, so setzen wir $\mathrm{E}(X, H) := \Delta(X, H)$. Dann ist $\mathrm{E}(X, H)$ eine Untergruppe von $\mathrm{E}(H)$.

Ist $\mathrm{E}(H) \neq \{1\}$, so setzen wir

$$\pi(H) := \big\{\mathrm{E}(P, H) \mid P \leq H,\ \mathrm{Rg}_L(P) = 1,\ \mathrm{E}(P, H) \neq \{1\}\big\}.$$

Da jedes Element von $\mathrm{E}(H)$ ein Zentrum hat und von 1 verschiedene Elemente aber auch nur eines, gilt

$$\mathrm{E}(H) = \bigcup_{\Xi \in \pi(H)} \Xi$$

und

$$\Xi \cap \Psi = \{1\},$$

falls nur Ξ und Ψ verschiedene Elemente von $\pi(H)$ sind. Dies bedeutet, dass $\pi(H)$ eine Partition von $\mathrm{E}(H)$ ist. Dabei nennen wir eine Menge π von nicht trivialen Untergruppe einer Gruppe G *Partition* von G, falls $G = \bigcup_{X \in \pi} X$ ist und sich zwei verschiedene Elemente von π stets trivial schneiden. Die Elemente von π heißen die *Komponenten* der Partition π. Die Partition π heißt *nicht trivial*, falls sie mehr als eine Komponente besitzt.

Wir werden sehen, dass die Gruppen $\mathrm{E}(H)$ und $\mathrm{E}(P)$ in allen uns interessierenden Fällen abelsch sind. Dies wird aus dem folgenden, allgemeineren Satz folgen.

1.13. Satz. *Es sei π eine nicht triviale Partition der Gruppe G. Genau dann ist G abelsch, wenn alle Komponenten von π Normalteiler von G sind. Ist G abelsch und enthält G ein von 1 verschiedenes Element endlicher Ordnung, so gibt es eine Primzahl p, so dass G eine elementarabelsche p-Gruppe ist.*

Beweis. Ist G abelsch, so sind alle Untergruppen von G normal in G, insbesondere also auch die Komponenten von π.

Es seien alle Komponenten von π normal in G. Ferner seien g und h zwei Elemente aus G und U, $V \in \pi$ mit $g \in U$ und $h \in V$. Weil V ein Normalteiler

ist, gilt h^{-1}, $g^{-1}hg \in V$. Also ist

$$h^{-1}g^{-1}hg \in V.$$

Analog folgt $h^{-1}g^{-1}h$, $g \in U$ und damit

$$h^{-1}g^{-1}hg \in U.$$

Ist nun $U \neq V$, so ist $U \cap V = \{1\}$, so dass $gh = hg$ ist. Es sei $U = V$. Da π nicht trivial ist, gibt es eine Komponente W von π, die von U verschieden ist. Es sei $1 \neq k \in W$. Da $gh \in U$ ist, folgt $ghk = kgh$. Nun ist $kg \notin U$, da sonst k in U läge. Also ist $kgh = hkg$. Insgesamt ist also

$$ghk = kgh = hkg = hgk.$$

Hieraus folgt, dass $gh = hg$ ist. Damit ist gezeigt, dass G abelsch ist.

Nun sei G abelsch. Enthält G ein Element endlicher Ordnung, so enthält G auch ein Element von Primzahlordnung p. Es sei g ein solches. Ferner sei $U \in \pi$ und $g \in U$. Es sei $h \in G - U$. Es gibt dann eine Komponente V von π mit $h \in V$. Dann ist $hg \notin V$, da $g \notin V$. Es gibt also eine von V verschiedene Komponente W mit $hg \in W$. Es folgt, da G abelsch ist,

$$h^p = h^p g^p = (hg)^p \in V \cap W = \{1\}.$$

Damit ist gezeigt, dass alle Elemente in $G - U$ die Ordnung p haben. Weil π nicht trivial ist, ist $G - U \neq \emptyset$, so dass G von $G - U$ erzeugt wird. Folglich ist G eine elementarabelsche p-Gruppe.

Ist κ eine Kollineation von L, so ist

$$\kappa^{-1}\mathrm{E}(X,H)\kappa = \mathrm{E}(X^\kappa, H^\kappa).$$

Ist $\kappa \in \Delta(H)$, so ist $X^\kappa = X$ und $H^\kappa = H$. Somit gilt

1.14. Satz. *Ist L ein irreduzibler projektiver Verband, ist H eine Hyperebene von L und ist $X \leq H$, so ist $\mathrm{E}(X,H)$ normal in $\Delta(H)$ und daher erst recht in $\mathrm{E}(H)$. Insbesondere ist $\mathrm{E}(P,H)$ für jeden Punkt P von H normal in $\mathrm{E}(H)$.*

Eine wichtige Folgerung aus diesem Satz ist das nächste Korollar.

1.15. Korollar. *Es sei H eine Hyperebene des irreduziblen projektiven Verbandes L. Ist $\mathrm{Rg}_L(H) \geq 3$, so ist $\mathrm{E}(H)$ abelsch. Ist $\mathrm{Rg}_L(H) = 2$, und ist $\pi(H)$ nicht trivial, so ist $\mathrm{E}(H)$ abelsch. In beiden Fällen folgt, dass $\mathrm{E}(H)$ eine elementarabelsche p-Gruppe ist, wenn $\mathrm{E}(H)$ ein von 1 verschiedenes Element endlicher Ordnung enthält.*

Ist L ein desarguesscher, irreduzibler projektiver Verband, so operiert die Gruppe $\mathrm{E}(H)$ auf der Menge der Punkte von L_H scharf transitiv, dh., zu je zwei Punkten P und Q, die nicht in H liegen, gibt es genau ein $\gamma \in \mathrm{E}(H)$ mit

$P^\gamma = Q$. Ist L endlich und ist n die Anzahl der Punkte von L_H, so ist also $n = |\mathrm{E}(H)|$. Nach I.7.6 ist, wenn r der Rang und q die Ordnung von L ist,

$$n = (q-1)^{-1}(q^r - 1 - q^{r-1} + 1) = q^{r-1}.$$

Andererseits ist $\mathrm{E}(H)$ endlich und daher nach 1.15 eine elementarabelsche p-Gruppe, so dass $\mathrm{E}(H)$ eine Potenz von p ist. Folglich ist q eine Potenz von p. Nennt man eine projektive Ebene L eine *Translationsebene*, wenn $\mathrm{E}(H)$ auf der Menge der Punkte von L_H transitiv operiert, so liefert der eben geführte Beweis auch noch, dass die Ordnung einer endlichen Translationsebene ebenfalls Potenz einer Primzahl ist. Es gilt also der im Anschluss an 7.7 in Kapitel I angekündigte

1.16. Satz. *Ist L ein endlicher, irreduzibler projektiver Verband mit $\mathrm{Rg}(L) \geq 4$ oder ist L eine endliche Translationsebene, so ist die Ordnung von L Potenz einer Primzahl.*

Da eine desarguessche projektive Ebene Translationsebene bez. jeder ihrer Geraden ist, ist auch die Ordnung einer endlichen desarguesschen Ebene Potenz einer Primzahl.

2. Der Kern von E(H)

Es sei L ein irreduzibler projektiver Verband mit $\mathrm{Rg}(L) \geq 3$ und H sei eine Hyperebene von L. Ist $\mathrm{Rg}(L) = 3$, so setzen wir voraus, dass L eine Translationsebene bez. H ist. Dann ist $\mathrm{E}(H)$ in jedem Falle abelsch. Mit $K(H)$ bezeichnen wir die Menge der Endomorphismen η von $\mathrm{E}(H)$, die die Eigenschaft haben, dass $\mathrm{E}(P,H)^\eta \subseteq \mathrm{E}(P,H)$ ist für alle Punkte P von H. Da offensichtlich die Summe, die Differenz und das Produkt zweier Elemente aus $K(H)$ wieder in $K(H)$ liegen, ist $K(H)$ ein Unterring des Endomorphismenringes von $\mathrm{E}(H)$. Man nennt $K(H)$ den *Kern* von $\mathrm{E}(H)$.

2.1. Satz. *Es sei L ein irreduzibler projektiver Verband mit $\mathrm{Rg}(L) \geq 3$ und H sei eine Hyperebene von L. Im Falle $\mathrm{Rg}(L) = 3$ sei L eine Translationsebene bez. H. Dann gilt: $K(H)$ ist ein Körper und $\mathrm{E}(H)$ ist ein Rechtsvektorraum über $K(H)$. Ist L desarguessch, was für $\mathrm{Rg}(L) > 3$ der Fall ist, so sind die Komponenten von $\pi(H)$ Unterräume des Ranges 1 des $K(H)$-Vektorraumes $\mathrm{E}(H)$. Ist P ein Punkt von L, der nicht in H liegt, so ist $\Delta(P,H)$ zur multiplikativen Gruppe von $K(H)$ isomorph.*

Beweis. Es sei $1 \neq \sigma \in \mathrm{E}(H)$ und $\eta \in K(H)$. Überdies gelte $\sigma^\eta = 1$. Nun sei $\tau \in \mathrm{E}(H)$ und das Zentrum Q von τ sei vom Zentrum P von σ verschieden. Weil σ genau ein Zentrum hat, folgt $\tau\sigma \notin \mathrm{E}(Q,H)$. Also ist $\tau\sigma \in \mathrm{E}(R,H)$, wobei R ein von Q verschiedener Punkt auf H ist. Hieraus folgt

$$\tau^\eta = \tau^\eta \sigma^\eta = (\tau\sigma)^\eta \in \mathrm{E}(Q,H) \cap \mathrm{E}(R,H) = \{1\},$$

so dass $\tau^\eta = 1$ ist für alle $\tau \in \mathrm{E}(H) - \mathrm{E}(P,H)$. Da diese Menge auf Grund unserer Annahme über L nicht leer ist und $\mathrm{E}(H)$ daher von ihr erzeugt wird, gilt $\mathrm{E}(H)^\eta = \{1\}$. Anders ausgedrückt: Jedes von Null verschiedene Element in $K(H)$ ist injektiv.

Wir zeigen als Nächstes, dass jedes von Null verschiedene Element aus $K(H)$ auch surjektiv ist. Dazu sei $1 \neq \sigma \in \mathrm{E}(P,H)$ und $1 \neq \tau \in \mathrm{E}(Q,H)$ sowie $P \neq Q$. Ferner sei X ein Punkt, der nicht in H liegt, und $0 \neq \eta \in K(H)$. Dann ist $\tau^\eta \neq 1$, wie wir gerade gesehen haben. Nun ist $\tau^\eta \in \mathrm{E}(Q,H)$. Daher ist $\sigma\tau^\eta \notin \mathrm{E}(P,H)$. Es sei etwa $\sigma\tau^\eta \in \mathrm{E}(R,H)$. Nach 1.12 sind die Punkte P, Q und R kollinear. Sie sind aber auch paarweise verschieden. Die Gerade $X+R$ liegt in der Ebene $P+Q+X$, da R ja auf $P+Q$ liegt. Weil diese Ebene durch das Zentrum Q von τ geht, bleibt sie unter τ fest, so dass auch die Gerade $X^\tau + P$ in $P+Q+X$ liegt. Weil die Geraden $X+R$ und $X^\tau+P$ nicht in H liegen, sind sie verschieden, so dass $(X+R)\cap(X^\tau+P)$ ein Punkt ist, der nicht auf $P+Q$ liegt. Somit ist

$$Y := \big(((X+R)\cap(X^\tau+P))+Q\big)\cap(X+P)$$

ein Punkt auf $P+X$. Weil Q das Zentrum von τ ist und P auf H liegt, folgt weiter

$$Y^\tau = \big(((X+R)\cap(X^\tau+P))+Q\big)\cap(X^\tau+P).$$

Hieraus folgt mittels des Modulargesetzes, dass

$$Y^\tau = (X+R)\cap(X^\tau+P) \leq X+R$$

ist.

Weil $\mathrm{E}(H)$ auf Grund unserer Annahme auf den Punkten des affinen Raumes L_H transitiv operiert, gibt es ein $\rho \in \mathrm{E}(P,H)$ mit $X^\rho = Y$. Es folgt

$$X^{\rho\tau} = Y^\tau \leq X+R.$$

Dies besagt, dass $\rho\tau \in \mathrm{E}(R,H)$ gilt. Dann ist aber auch $\rho^\eta\tau^\eta = (\rho\tau)^\eta \in \mathrm{E}(R,H)$. Ferner ist $\sigma\rho^{-\eta} \in E(P,H)$, da σ, $\rho^\eta \in \mathrm{E}(P,H)$ gilt. Also ist

$$\sigma\rho^{-\eta} = \sigma\tau^\eta\tau^{-\eta}\rho^{-\eta} \in \mathrm{E}(P,H)\cap\mathrm{E}(R,H) = \{1\}.$$

Folglich ist $\sigma = \rho^\eta$, so dass η in der Tat surjektiv ist. Damit ist gezeigt, dass die von Null verschiedenen Elemente aus $K(H)$ Automorphismen sind. Da ihre Inversen offenbar auch zu $K(H)$ gehören, ist $K(H)$ als Körper erkannt. Insbesondere ist $\mathrm{E}(H)$ damit ein Rechtsvektorraum über seinem Kern.

Es sei P ein Punkt, der nicht in H liegt, und δ sei ein Element aus $\Delta(P,H)$. Dann ist die durch $\tau^{\delta^*} := \delta^{-1}\tau\delta$ für $\tau \in \mathrm{E}(H)$ erklärte Abbildung δ^* nach 1.14 ein Automorphismus von $\mathrm{E}(H)$, der sogar in $K(H)$ liegt. Ist η ebenfalls in $\Delta(P,H)$ und ist $\delta^* = \eta^*$, so ist $\delta^{-1}\tau\delta = \eta^{-1}\tau\eta$ für alle $\tau \in \mathrm{E}(H)$. Hieraus folgt, dass $\eta\sigma^{-1}$ im Zentralisator von $\mathrm{E}(H)$ liegt, dh., dass $\eta\delta^{-1}$ mit allen Elementen von $\mathrm{E}(H)$ vertauschbar ist. Weil $\eta\delta^{-1}$ den Fixpunkt P hat und $\mathrm{E}(H)$ auf der Menge der Punkte von L_H transitiv operiert, lässt $\eta\delta^{-1}$ alle Punkte von L_H fest. Folglich ist $\eta\delta^{-1} = 1$, so dass die Abbildung $*$ injektiv ist. Somit ist $*$ ein Monomorphismus von $\Delta(P,H)$ in die multiplikative Gruppe von $K(H)$.

Wir zeigen, dass die Abbildung $*$ auch surjektiv ist. Dazu sei $0 \neq \eta \in K(H)$. Wir definieren die Abbildung σ wie folgt. Es sei Q ein Punkt von L_H. Es gibt

dann genau ein $\tau \in \mathrm{E}(H)$ mit $P^\tau = Q$. Wir setzen $Q^\sigma := P^{\tau^\eta}$. Dann ist σ eine Abbildung der Menge der Punkte von L_H in sich. Mittels η^{-1} definieren wir auf die gleiche Weise eine Abbildung σ'. Dann ist

$$P^{\tau\sigma\sigma'} = (P^{\tau^\eta})^{\sigma'} = P^{\tau^{\eta\eta^{-1}}} = P^\tau = P^{\tau^{\eta^{-1}\eta}} = P^{\tau\sigma'\sigma},$$

so dass also $\sigma\sigma' = 1 = \sigma'\sigma$ ist. Somit ist σ bijektiv und $\sigma^{-1} = \sigma'$.

Es seien Q, R und S drei kollineare Punkte von L_H. Es gibt dann ein $\rho \in \mathrm{E}(H)$ mit $Q^\rho = P$. Die Punkte P, R^ρ und S^ρ sind dann ebenfalls kollinear. Es gibt λ, $\mu \in \mathrm{E}(H)$ mit $P^\lambda = R^\rho$ und $P^\mu = S^\rho$. Wegen der Kollinearität von P, R^ρ und S^ρ folgt, dass λ und μ das gleiche Zentrum haben. Dann haben aber auch λ^η und μ^η das gleiche Zentrum. Es folgt, dass auch die Punkte P, P^{λ^η} und P^{μ^η} kollinear sind. Nun ist aber $Q^{\rho\sigma} = P^\sigma = P$, $R^{\rho\sigma} = P^{\lambda^\eta}$ und $S^{\rho\sigma} = P^{\mu^\eta}$. Also sind auch die Punkte $Q^{\rho\sigma}$, $R^{\rho\sigma}$ und $S^{\rho\sigma}$ kollinear. Wir wissen bereits, dass $\sigma^{-1}\ \rho^{-1}\ \sigma \in \mathrm{E}(H)$ ist. Daher sind auch die Punkte $Q^{\rho\sigma\sigma^{-1}\rho^{-1}\sigma} = Q^\sigma$, $R^{\rho\sigma\sigma^{-1}\rho^{-1}\sigma} = R^\sigma$, $S^{\rho\sigma\sigma^{-1}\rho^{-1}\sigma} = S^\sigma$ kollinear. Da σ^{-1} eine Abbildung gleicher Bauart wie σ ist, bildet auch σ^{-1} kollineare Punkte auf kollineare Punkte ab. Aus I.8.8 folgt daher, falls jede Gerade von L wenigstens drei Punkte trägt, dass σ durch genau eine Kollineation von L induziert wird, die, da σ alle Geraden durch P festlässt, in $\Delta(P, H)$ liegt. Enthalten alle Geraden von L genau drei Punkte, so ist $|\mathrm{E}(Q, H)| = 2$ für alle Punkte Q von H. Dann ist aber auch $|K(H)| = 2$, so dass in diesem Falle nichts zu beweisen ist. Damit ist gezeigt, dass $*$ ein Isomorphismus von $\Delta(P, H)$ auf die multiplikative Gruppe von $K(H)$ ist.

Die Gruppen $\mathrm{E}(Q, H)$ sind Unterräume des $K(H)$-Vektorraumes $\mathrm{E}(H)$. Ist L desarguessch, so müssen wir noch zeigen, dass sie alle den Rang 1 haben. Es sei also L desarguessch. Sind σ und τ von 1 verschiedene Elemente aus $\mathrm{E}(Q, H)$ und ist P ein Punkt, der nicht in H liegt, so ist $P \neq P^\sigma$, P^τ und $P + P^\sigma = P + P^\tau$. Es gibt also ein $\delta \in \Delta(P, H)$ mit $P^{\sigma\delta} = P^\tau$. Nun ist $P^{\delta^{-1}} = P$ und $\delta^{-1}\sigma\delta \in E(H)$. Aus

$$P^\tau = P^{\sigma\delta} = P^{\delta^{-1}\sigma\delta}$$

folgt daher, dass

$$\sigma^{\delta^*} = \delta^{-1}\sigma\delta = \tau$$

ist. Damit ist gezeigt, dass die $\mathrm{E}(Q, H)$ Unterräume des Ranges 1 sind, falls L desarguessch ist. Hiermit ist 2.1 in allen seinen Teilen bewiesen.

2.2. Korollar. *Ist L ein endlicher, desarguesscher irreduzibler projektiver Verband der Ordnung q und ist H eine Hyperebene von L, so ist $K(H) \cong \mathrm{GF}(q)$.*

Beweis. Dies folgt sofort aus $|K(H)| = q$ und aus der Tatsache, dass es bis auf Isomorphie nur einen endlichen Körper mit q Elementen gibt, nämlich das Galoisfeld $\mathrm{GF}(q)$.

2.3. Korollar. *Es sei L ein endlicher, irreduzibler projektiver Verband und H sei eine Hyperebene. Ferner sei L eine Translationsebene bez. H, falls* $\mathrm{Rg}(L) = 3$ *ist. Ist dann P ein Punkt von L_H, so ist $\Delta(P, H)$ zyklisch.*

Beweis. In diesen Fällen ist $K(H)$ ein endlicher Körper, so dass die multiplikative Gruppe von $K(H)$ nach bekannten Sätzen zyklisch ist.

2.4. Satz. *Es sei L ein irreduzibler, desarguesscher projektiver Verband und Σ sei eine Untergruppe von $\mathrm{E}(H)$. Genau dann ist Σ ein Unterraum des $K(H)$-Vektorraumes $\mathrm{E}(H)$, wenn es ein $X \in L$ gibt mit $X \leq H$ und $\Sigma = \mathrm{E}(X, H)$.*

Beweis. Aus der Definition von $K(H)$ folgt, dass $\mathrm{E}(X, H)$ für alle $X \in L$ mit $X \leq H$ ein Unterraum des $K(H)$-Vektorraumes $\mathrm{E}(H)$ ist.

Es sei also umgekehrt Σ ein Unterraum des Vektorraumes $\mathrm{E}(H)$. Ferner sei S die Menge der Zentren der von 1 verschiedenen Elemente aus Σ. Schließlich sei $X := \Sigma_{P \in S} P$. Ist $S = \emptyset$, so ist $X = 0$ und $\Sigma = \{1\}$, so dass $\Sigma = \mathrm{E}(0, H)$ ist. Es sei also $S \neq \emptyset$. Sicherlich ist $\Sigma \subseteq \mathrm{E}(X, H)$. Wir müssen also zeigen, dass $\mathrm{E}(X, H) \subseteq \Sigma$ ist. Dazu genügt es zu zeigen, dass S alle Punkte von X enthält. Ist nämlich P ein Punkt von X, der in S liegt, so ist $\mathrm{E}(P, H) \cap \Sigma \neq \{1\}$. Hieraus folgt mit 2.1, da L als desarguessch vorausgesetzt wurde, dass $\mathrm{E}(P, H) \subseteq \Sigma$ gilt. Um nun zu zeigen, dass S alle Punkte von X enthält, genügt es nach I.2.12 zu zeigen, dass mit zwei verschiedenen Punkten auch alle Punkte ihrer Verbindungsgeraden in S liegen.

Es seien also P und Q zwei verschiedene Punkte von S. Dann ist, wie wir bereits bemerkten, $\mathrm{E}(P, H) \subseteq \Sigma$ und $\mathrm{E}(Q, H) \subseteq \Sigma$. Also ist auch

$$\mathrm{E}(P, H)E(Q, H) \subseteq \Sigma.$$

Es sei R ein von P und Q verschiedener Punkt auf $P + Q$. Schließlich sei U ein Punkt von L_H und $1 \neq \tau \in \mathrm{E}(R, H)$. Wir setzen $V := (U^\tau + Q) \cap (U + P)$ und $W := (U^\tau + P) \cap (U + Q)$. Es gibt dann ein $\rho \in \mathrm{E}(P, H)$ mit $U^\rho = V$ und ein $\sigma \in \mathrm{E}(Q, H)$ mit $U^\sigma = W$. Dann ist aber $U^{\rho\sigma} = U^\tau$ und folglich $\tau = \rho\sigma$. Somit ist $1 \neq \tau \in \Sigma$, was wiederum $R \in S$ nach sich zieht.

3. Pappossche Geometrien

In diesem und dem nächsten Abschnitt werden wir der Frage nachgehen, in welchen projektiven Geometrien der Satz von Pappos gilt. Dabei werden wir in diesem Abschnitt nur den Fall der desarguesschen Geometrien betrachten, der ja sicher dann vorliegt, wenn die betrachteten Geometrien mindestens den Rang 4 haben. Im nächsten Abschnitt werden wir den Satz von Hessenberg beweisen, der besagt, dass eine pappossche projektive Ebene stets auch desarguessch ist.

Es sei L ein irreduzibler, desarguesscher projektiver Verband, in dem der Satz von Pappos gelte. Es sei H eine Hyperebene und P ein Punkt von L, der auch auf H liegen darf. Weiter seien δ und η zwei von 1 verschiedene Elemente aus $\Delta(P, H)$ und G und K seien zwei verschiedene Geraden durch P, die nicht in H liegen. Schließlich sei X ein von P und $G \cap H$ verschiedener Punkt auf G und Y ein von P und $K \cap H$ verschiedener Punkt auf K. Ist $\delta = \eta$, so ist $\delta\eta = \eta\delta$. Es sei also $\delta \neq \eta$. Dann sind Y, Y^δ und Y^η drei verschiedene Punkte auf K, die alle von P verschieden sind. Ebenso sind X^δ, X^η und $X^{\delta\eta}$

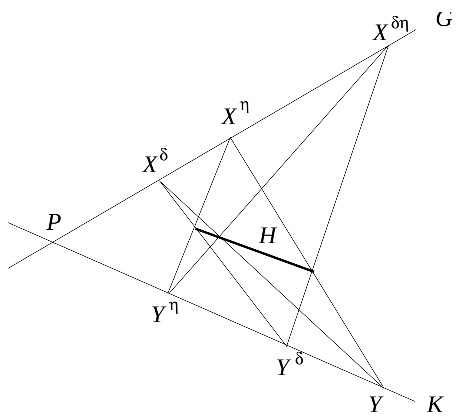
drei verschiedene Punkte auf G, die auch von P verschieden sind. Weil wir die Gültigkeit des Satzes von Pappos vorausgesetzt haben, sind die Punkte

$$(X^\delta + Y^\delta) \cap (X^\eta + Y^\eta),$$
$$(X^\delta + Y) \cap (X^{\delta\eta} + X^\eta),$$
$$(X^{\delta\eta} + Y^\delta) \cap (X^\eta + Y)$$

kollinear. Nun ist

$$(X^\delta + Y^\delta) \cap H = (X + Y) \cap H = (X^\eta + Y^\eta) \cap H,$$

so dass der erste dieser Punkte auf H liegt. Der zweite Punkt liegt aus dem



gleichen Grund auf H. Somit auch der dritte. Nun ist

$$X^{\eta\delta} = \big(((X^\eta + Y) \cap H) + Y^\delta\big) \cap G.$$

Aus der gerade gemachten Bemerkung folgt, dass

$$\big((X^\eta + Y) \cap H\big) + Y^\delta = Y^\delta + X^{\delta\eta}$$

ist. Also ist

$$X^{\eta\delta} = (Y^\delta + X^{\delta\eta}) \cap G = X^{\delta\eta}.$$

Hieraus folgt schließlich, dass $\delta\eta = \eta\delta$ ist. Somit ist $\Delta(P, H)$ abelsch.

Es sei nun umgekehrt $\Delta(P, H)$ abelsch für alle Punkt-Hyperebenenpaare des desarguesschen projektiven Verbandes L. (Wie wir wissen, ist $\Delta(P, H)$ sicher dann abelsch, wenn P auf H liegt.) Es seien G und K zwei verschiedene Geraden durch P und P_1, P_2 und P_3 seien drei verschiedene Punkte auf G, die alle von P verschieden seien. Entsprechend seien Q_1, Q_2 und Q_3 drei verschiedene Punkte auf K, die ebenfalls von P verschieden seien. Schließlich sei

$$J := \big((P_1 + Q_2) \cap (Q_1 + P_2)\big) + \big((P_1 + Q_3) \cap (Q_1 + P_3)\big).$$

Dann ist J eine Gerade in der Ebene $G+K$. Es sei A ein Komplement von $G+K$. Dann ist $H := J + A$ eine Hyperebene von L mit $H \cap (G + K) = J$. Hieraus

folgt, dass die Punkte P_i und Q_j nicht in H liegen. Es gibt δ, $\eta \in \Delta(P,H)$ mit $Q_3^\delta = Q_2$ und $Q_3^\eta = Q_1$. Setze

$$X := \big(Q_3 + ((P_1 + Q_2) \cap (Q_1 + P_2))\big) \cap G.$$

Weil die Gerade G durch P geht und der Punkt $(P_1 + Q_2) \cap (Q_1 + P_2)$ auf H liegt, folgt mit Hilfe des Modulargesetzes

$$\begin{aligned} X^\delta &= \big(Q_3^\delta + ((P_1 + Q_2) \cap (Q_1 + P_2))\big) \cap G \\ &= \big(Q_2 + ((P_1 + Q_2) \cap (Q_1 + P_2))\big) \cap G \\ &= (P_1 + Q_2) \cap (Q_2 + Q_1 + P_2) \cap G \\ &= (P_1 + Q_2) \cap G \\ &= P_1. \end{aligned}$$

Ebenso folgt

$$\begin{aligned} X^\eta &= \big(Q_3^\eta + ((P_1 + Q_2) \cap (Q_1 + P_2))\big) \cap G \\ &= \big(Q_1 + ((P_1 + Q_2) \cap (Q_1 + P_2))\big) \cap G \\ &= (Q_1 + P_2) \cap (Q_1 + P_1 + Q_2) \cap G \\ &= (Q_1 + P_2) \cap G \\ &= P_2 \end{aligned}$$

und

$$\begin{aligned} P_1^\eta &= \big(Q_3^\eta + ((P_1 + Q_3) \cap (Q_1 + P_3))\big) \cap G \\ &= \big(Q_1 + ((P_1 + Q_3) \cap (Q_1 + P_3))\big) \cap G \\ &= (Q_1 + P_3) \cap (Q_1 + P_1 + Q_3) \cap G \\ &= (Q_1 + P_3) \cap G \\ &= P_3 \end{aligned}$$

Es ist also $X^\delta = P_1$, $X^\eta = P_2$ und $X^{\delta\eta} = P_1^\eta = P_3$. Nun ist $\delta\eta = \eta\delta$, woraus folgt, dass

$$P_2^\delta = X^{\eta\delta} = X^{\delta\eta} = P_3$$

ist. Daraus folgt wiederum, dass $(P_2 + Q_3) \cap (Q_2 + P_3)$ ein Punkt von H ist. Also ist

$$(P_2 + Q_3) \cap (Q_2 + P_3) \leq H \cap (G + K) = J,$$

so dass in L der Satz von Pappos gilt. Damit ist ein Teil des folgenden Satzes bewiesen.

3.1. Satz. *Ist L ein irreduzibler, desarguesscher projektiver Verband mit* $\mathrm{Rg}(L) \geq 3$, *so sind die folgenden Bedingungen äquivalent:*
(a) *In L gilt der Satz von Pappos.*
(b) *$\Delta(P,H)$ ist für alle Punkt-Hyperebenenpaare (P,H) abelsch.*
(c) *Es gibt ein nicht inzidentes Punkt-Hyperebenenpaar (P,H), so dass $\Delta(P,H)$ abelsch ist.*
(d) *Es gibt eine Hyperebene H, so dass $K(H)$ kommutativ ist.*

Beweis. Die Äquivalenz von (a) und (b) haben wir gerade bewiesen und die Äquivalenz von (c) und (d) folgt aus Satz 2.1. Bedingung (c) ist natürlich eine Folge von (b). Es bleibt zu zeigen, dass (b) eine Folge von (c) ist. Um dies zu zeigen, beweisen wir zunächst, dass die von allen $\mathrm{E}(H)$ erzeugte Gruppe auf der Menge der nicht inzidenten Punkt-Hyperebenenpaare transitiv operiert.

Es seien H und K zwei verschiedene Hyperebenen von L. Dann ist $H \cap K$ eine Ko-Gerade von L. Es gibt also eine Gerade G mit $\Pi = G \oplus (H \cap K)$. Weil G mindestens drei Punkte trägt, gibt es einen Punkt P auf G, der weder auf H noch auf K liegt. Setze $V := P + (H \cap K)$. Dann ist V eine Hyperebene. Weil L desarguessch ist, gibt es ein $\tau \in \mathrm{E}(P, V)$ mit $(G \cap H)^\tau = G \cap K$. Es folgt, dass $H^\tau = K$ ist. Die fragliche Gruppe ist also auf der Menge der Hyperebenen transitiv. Weil $\mathrm{E}(H)$ auf der Menge der Punkte von L_H transitiv operiert, ist die fragliche Gruppe auf der Menge der nicht inzidenten Punkt-Hyperebenenpaare transitiv.

Sei nun (P, H) ein nicht inzidentes Punkt-Hyperebenenpaar und die Gruppe $\Delta(P, H)$ sei abelsch. Ist (Q, K) ein weiteres, nicht inzidentes Punkt-Hyperebenenpaar, so gibt es also eine Kollineation γ mit $P^\gamma = Q$ und $H^\gamma = K$. Es folgt

$$\gamma^{-1}\Delta(P, H)\gamma = \Delta(P^\gamma, H^\gamma) = \Delta(Q, K),$$

so dass auch $\Delta(Q, K)$ abelsch ist.

Da die Gruppen $\mathrm{E}(P, H)$ für alle inzidenten Punkt-Hyperebenenpaare stets abelsch sind, ist alles bewiesen.

Unsere Zwischenbemerkung ist wichtig genug, um als Satz formuliert zu werden.

3.2. Satz. *Ist L ein irreduzibler, desarguesscher projektiver Verband, so ist die von allen Elationen erzeugte Untergruppe der Kollineationsgruppe von L auf der Menge der nicht inzidenten Punkt-Hyperebenenpaare von L transitiv.*

Aus 3.1 und 3.2 folgt noch das

3.3. Korollar. *In allen endlichen, desarguesschen irreduziblen projektiven Geometrien gilt der Satz von Pappos.*

Alle Beweise von 3.3, die ich kenne, benutzen den Satz von Wedderburn, dass alle endlichen Körper kommutativ sind. Einen geometrischen Beweis zu finden, scheint also sehr schwierig zu sein. Den Beweis von Tecklenburg 1987 kann ich nicht als einen solchen werten, da er nur den einfachen wittschen Beweis des wedderburnschen Satzes in eine komplizierte geometrische Sprache übersetzt.

4. Der Satz von Hessenberg

Hessenberg zeigt, wenn auch mit einigen Lücken im Beweis, dass papposche projektive Ebenen auch desarguessch sind (Hessenberg 1905). Sein Beweis und einige andere sind in Pickerts Buch abgedruckt. Diese Beweise haben jedoch niemanden so recht befriedigt, da sie wegen der vielen zu betrachtenden Entartungsfälle sehr unübersichtlich sind. Entartungsfälle in algebraischen Situationen sind meist banal, während sie in geometrischen Situationen häufig sehr

viel Kopfzerbrechen bereiten. Gesucht war also ein Beweis, bei dem man schon früh von algebraischen Methoden Gebrauch machen konnte. Vorbild war der Satz von Baer, dass die Gültigkeit des (P, G)-Satzes von Desargues der (P, G)-Transitivität der fraglichen Ebene äquivalent ist. Einen ersten Beweis dieser Art fand ich im Jahre 1968, den ich eine Weile als den schönsten Beweis für den hessenbergschen Satz ansah (Lüneburg 1969b). Dann jedoch publizierte A. Herzer seinen Beweis dieses Satzes (Herzer 1972). Dieser Beweis zählt für mich zu den mathematischen Juwelen. Ich werde ihn also, Altruist der ich bin, dem Leser nicht vorenthalten.

Vom geometrischen Standpunkt her gesehen sind Kollineationen mit vielen Fixpunkten einfacher zu handhaben als solche ohne Fixpunkte. Das lassen schon unsere Sätze über Perspektivitäten ahnen. Antiautomorphismen eines projektiven Verbandes haben keine Fixpunkte. Dennoch gibt es auch hier Punkte, die vor anderen ausgezeichnet sind. Bevor wir sie definieren, verabreden wir noch, dass Antiautomorphismen eines projektiven Verbandes in Zukunft *Korrelationen* oder auch *Dualitäten* genannt werden.

Es sei κ eine Korrelation des projektiven Verbandes L. Der Punkt P von L heißt *absolut*, falls $P \leq P^\kappa$ gilt. Analog heißt die Hyperebene H von L *absolut*, wenn $H^\kappa \leq H$ ist.

4.1. Satz. *Es sei κ eine Korrelation der projektiven Ebene L. Sind P und Q zwei verschiedene absolute Punkte von κ und gilt $Q \leq P^\kappa$, so sind P und Q die einzigen absoluten Punkte auf P^κ. Überdies ist $P^{\kappa^2} = Q$ und $\kappa^2 \neq 1$.*

Beweis. Setze $G := P^\kappa$. Die Menge der Geraden durch P wird von κ bijektiv auf die Menge der Punkte von G abgebildet. Da G nach Voraussetzung mindestens zwei absolute Punkte trägt, gibt es eine von G verschiedene Gerade H durch P, so dass H^κ ein absoluter Punkt auf G ist, so dass also $H^\kappa \leq H^{\kappa^2}$ gilt. Hieraus folgt, da auch K^{-1} eine Korrelation ist, dass

$$(H^{\kappa^2})^{\kappa^{-1}} \leq (H^\kappa)^{\kappa^{-1}},$$

dh., dass

$$H^\kappa \leq H$$

ist. Also ist

$$H^\kappa = H \cap G = P.$$

Dies besagt, dass es nur eine von G verschiedene Gerade durch P gibt, deren Bild unter κ ein absoluter Punkt auf G ist, nämlich die Gerade $P^{\kappa^{-1}}$. Weil Q ein zweiter absoluter Punkt auf G ist, ist also $G^\kappa = Q$. Hieraus folgt weiter

$$P^{\kappa^2} = G^\kappa = Q.$$

Weil schließlich $P \neq Q$ ist, ist $\kappa^2 \neq 1$. Damit ist alles bewiesen.

Es sei κ eine Korrelation der projektiven Ebene L und G und H seien zwei verschiedene Geraden von L. Die Korrelation κ heiße (G, H)-*Korrelation*, falls die Punkte von G wie auch die Punkte von H absolute Punkte von κ sind. Es gilt nun der folgende Satz.

4.2. Satz. *Es seien G und H zwei verschiedene Geraden der projektiven Ebene L und κ sei eine (G,H)-Korrelation von L. Es seien ferner P und Q die beiden verschiedenen Punkte von L mit $P^\kappa = G$ und $Q^\kappa = H$. Schließlich sei $S := G \cap H$ und $V := P + Q$. Dann gilt:*

a) *$P \not\leq G$ und $Q \not\leq H$.*

b) *Ist X eine Gerade durch P, so ist X absolut und $X^\kappa = X \cap G$. Ist Y eine Gerade durch Q, so ist Y absolut und $Y^\kappa = Y \cap H$.*

c) *Ist X ein Punkt von L_V, so ist*

$$X^\kappa = \big((X+P) \cap G\big) + \big((X+Q) \cap H\big).$$

d) *Es ist $S \leq V$.*

e) *Es ist $G^\kappa = Q$ und $H^\kappa = P$.*

f) *Es ist $S^\kappa = V$ und $V^\kappa = S$.*

g) *Ist X eine Gerade mit $S \not\leq X$, so ist*

$$X^\kappa = \big((X \cap G) + Q\big) \cap \big((X \cap H) + P\big).$$

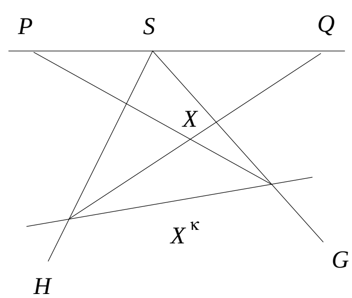
h) *Durch P, Q, G und H wird κ eindeutig festgelegt.*

i) *Ist A ein absoluter Punkt von κ, so ist $A \leq G$ oder $A \leq H$.*

Beweis. a) Weil G mindestens drei Punkte trägt und alle diese Punkte absolut sind, folgt mit 4.1 wegen $P^\kappa = G$, dass P nicht auf G liegt. Ebenso folgt, dass Q nicht auf H liegt.

b) Es sei X eine Gerade durch P. Dann ist $X^\kappa \leq P^\kappa = G$, so dass X^κ nach Voraussetzung absolut ist. Also ist $X^\kappa \leq X^{\kappa^2}$. Anwendung von κ^{-1} zeigt, dass $X^\kappa \leq X$ ist. Somit ist X absolut. Wegen $X^\kappa \leq G$ und $X^\kappa \leq X$ folgt schließlich $X^\kappa = X \cap G$. Ebenso folgt die Aussage über Y.

c) Es sei X ein Punkt, der nicht auf V liegt. Wegen $V = P + Q$ ist dann



$X = (X+P) \cap (X+Q)$. Mit b) folgt daher

$$X^\kappa = (X+P)^\kappa + (X+Q)^\kappa = \big((X+P) \cap G\big) + \big((X+Q) \cap H\big).$$

d) Wäre $S \not\leq V$, so folgte mit c) der Widerspruch

$$S^\kappa = \big((S+P) \cap G\big) + \big((S+Q) \cap H\big) = S + S = S.$$

e) Mit a) folgt $V \neq G$, so dass nach d) gilt, dass $S = G \cap V$ ist. Ist nun X ein von S verschiedener Punkt auf G, so ist also $X \not\leq V$. Nach c) und dem Modulargesetz ist also

$$X^\kappa = \big((X+P) \cap G\big) + \big((X+Q) \cap H\big) = X + \big((X+Q) \cap H\big) = X + Q.$$

Ist nun Y ein weitere von X und S verschiedener Punkt auf G, so folgt, wie gerade gesehen, $Y^\kappa = Y + Q$ und daher

$$G^\kappa = (X+Y)^\kappa = X^\kappa \cap Y^\kappa = (X+Q) \cap (Y+Q) = Q.$$

ebenso folgt, dass $H^\kappa = P$ ist.

f) Es ist

$$S^\kappa = (G \cap H)^\kappa = G^\kappa + H^\kappa = Q + P = V.$$

Entsprechend gilt

$$V^\kappa = (P+Q)^\kappa = P^\kappa \cap Q^\kappa = G \cap H = S.$$

g) Ist X eine Gerade, die nicht durch S geht, so ist $X = (X \cap G) + (X \cap H)$. Daher ist

$$X^\kappa = (X \cap G)^\kappa \cap (X \cap H)^\kappa = \big((X \cap G) + Q\big) \cap \big((X \cap H) + P\big).$$

h) Es sei λ eine weitere (G,H)-Korrelation mit $P^\lambda = G$ und $Q^\lambda = H$. Nach c) gilt dann die Gleichung $X^\kappa = X^\lambda$ für alle Punkte X von L_V. Daher gilt $X^{\kappa\lambda^{-1}} = X$ für alle diese Punkte. Nach I.8.8 ist daher $\kappa\lambda^{-1} = 1$, so dass in der Tat $\kappa = \lambda$ ist. Es sei A ein absoluter Punkt von κ. Ist $A \leq V$, so ist $S = V^\kappa \leq A^\kappa$. Wäre $A \neq S$, so folgte $A^\kappa \neq S^\kappa = V$. Weil A absolut ist, folgte weiter $A = A^\kappa \cap V = S$. Also ist doch $A = S$. Es sei also $A \not\leq V$. Dann ist

$$A \leq A^\kappa = \big((A+P) \cap G\big) + \big((A+Q) \cap H\big).$$

Wir dürfen annehmen, dass A nicht auf G liegt. Dann ist A ein von $(A+P) \cap G$ verschiedener Punkt auf A^κ. Es ist also $A^\kappa = A + ((A+P) \cap G)$. Mittels des Modulargesetzes folgt weiter

$$A^\kappa = (A+P) \cap (A+G) = A + P.$$

Also gilt $(A+Q) \cap H \leq A + P$. Weil A nicht auf V liegt, ist $A + P \neq A + Q$. Daher ist

$$(A+Q) \cap H = (A+P) \cap (A+Q) = A,$$

so dass A in der Tat auf H liegt.

Die zweite Aussage von i) ist dual zur ersten. Damit ist der Satz vollständig bewiesen.

Hier nun der alles entscheidende Satz von Herzer, der die Verbindung des Satzes von Pappos zu den (G,H)-Korrelationen herstellt.

4.3. Satz. *Ist L eine projektive Ebene, so sind die beiden folgenden Aussagen äquivalent:*
1) *In L gilt der Satz von Pappos.*
2) *Sind G und H zwei verschiedene Geraden und P und Q zwei verschiedene Punkte von L, gilt ferner $P, Q \not\leq G, H$ und sind die Punkte P, Q und $G \cap H$ kollinear, so gibt es eine (G, H)-Korrelation κ von L mit $P^\kappa = G$ und $Q^\kappa = H$.*

Beweis. 1) impliziert 2): Es seien P und Q zwei Punkte und G und H zwei Geraden von L, die die Voraussetzungen von 2) erfüllen. Setze $V := P + Q$ und $S := G \cap H$. Setze ferner

$$L_{S,V} := L_V \cap (L^d)_S.$$

Dann besteht $L_{S,V}$ also aus den Punkten, die nicht auf V liegen, und den Geraden, die nicht durch S gehen. Wir definieren zwei Abbildungen κ und λ von $L_{S,V}$ in sich wie folgt: ist X ein Punkt von $L_{S,V}$, so setzen wir

$$X^\kappa := \big((X + P) \cap G\big) + \big((X + Q) \cap H\big)$$

und ist X eine Gerade von L_S, V, so setzen wir

$$X^\kappa := \big((X + P) \cap G\big) + \big((X + Q) \cap H\big)$$

und ist X eine Gerade von $L_{S,V}$, so setzen wir

$$X^\kappa := \big((X \cap G) + Q\big) \cap \big((X \cap H) + P\big).$$

Ist Y ein Punkt von $L_{S,V}$, so setzen wir ferner

$$Y^\lambda := \big((Y + Q) \cap G\big) + \big((Y + P) \cap H\big).$$

Schließlich setzen wir

$$Y^\kappa := \big((Y \cap G) + P\big) \cap \big((Y \cap H) + Q\big),$$

falls Y eine Gerade von $L_{S,V}$ ist.

Ist X ein Punkt von $L_{S,V}$, so folgt mittels des Modulargesetzes $X^\kappa \cap G = (X + P) \cap G$ und $X^\kappa \cap H = (X + Q) \cap H$. Hieraus folgt weiter

$$X^\kappa \cap G) + P = \big((X + P) \cap G\big) + P = X + P$$

und

$$X^\kappa \cap H) + Q = \big((X + Q) \cap H\big) + Q = X + Q.$$

Daher ist

$$X^{\kappa\lambda} = \big((X^\kappa \cap G) + P\big) \cap \big((X^\kappa \cap H) + Q\big) = (X + P) \cap (X + Q) = X.$$

Ist X eine Gerade von $L_{S,V}$, so folgt mittels des Modulargesetzes $X^\kappa + P = (X \cap H) + P$ und $X^\kappa + Q = (X \cap G) + Q$. Hieraus folgt weiter

$$(X^\kappa + P) \cap H = X \cap H$$

und

$$(X^\kappa + Q) \cap G = X \cap G.$$

Somit ist

$$X^{\kappa\lambda} = \big((X^\kappa + Q) \cap G\big) + \big((X^\kappa + P) \cap H\big) = (X \cap G) + (X \cap H) = X.$$

Also ist $\kappa\lambda = 1$. Aus Dualitätsgründen, — den Satz von Pappos haben wir ja noch nicht benutzt —, ist dann auch $\lambda\kappa = 1$, so dass κ eine Bijektion von $L_{S,V}$ auf sich und dass λ die zu κ inverse Abbildung ist.

Es sei X ein Punkt und Y eine Gerade von $L_{S,V}$ und es gelte $X \leq Y$. Wir zeigen, dass $Y^\kappa \leq X^\kappa$ gilt. Es sei zunächst $X \leq G$. Dann folgt unter Benutzung des Modulargesetzes

$$\begin{aligned} X^\kappa &= \big((X + P) \cap G\big) + \big((X + Q) \cap H\big) \\ &= X + \big((X + Q) \cap H\big) \\ &= (X + Q) \cap (X + H) = X + Q. \end{aligned}$$

Andererseits ist, da ja $Y \cap G = X$ ist,

$$Y^\kappa = \big((Y \cap G) + Q\big) \cap \big((Y \cap H) + P\big) = (X + Q) \cap \big((Y \cap H) + P\big),$$

so dass in diesem Falle $Y^\kappa \leq X + Q = X^\kappa$ gilt. Liegt X auf H, so folgt genauso, dass $Y^\kappa \leq X^\kappa$ ist. Die Fälle, dass P oder Q auf Y liegen, sind dual zu den behandelten, so dass auch hier $Y^\kappa \leq X^\kappa$ gilt, da wir den Satz von Pappos noch immer nicht benutzt haben.

Wir dürfen daher des Weiteren annehmen, dass X weder auf G noch auf H liegt und dass Y weder durch P noch durch Q geht. Dann sind die Punkte P, S und Q drei verschiedene Punkte auf V, die von $V \cap Y$ verschieden sind. Ferner sind $Y \cap G$, X und $Y \cap H$ drei verschiedene Punkte auf Y, die ebenfalls von $V \cap Y$ verschieden sind. Weil in L der Satz von Pappos gilt, sind daher die Punkte

$$\begin{gathered} \big((Y \cap G) + Q\big) \cap \big((Y \cap H) + P\big), \\ (X + P) \cap \big((Y \cap G) + S\big), \\ (X + Q) \cap \big((Y \cap H) + S\big) \end{gathered}$$

kollinear. Wegen $(Y \cap G) + S = G$ und $(Y \cap H) + S = H$ folgt daher, dass der Punkt

$$Y^\kappa = \big((Y \cap G) + Q\big) \cap \big((Y \cap H) + P\big)$$

auf der Geraden

$$\big((X + P) \cap G\big) + \big((X + Q) \cap H\big) = X^\kappa$$

liegt. Aus $X \leq Y$ folgt also stets $Y^\kappa \leq X^\kappa$.

Da λ von gleicher Bauart ist — es haben ja nur P und Q ihre Rollen vertauscht —, gilt auch für λ, dass $Y^\lambda \leq X^\lambda$ eine Folge von $X \leq Y$ ist. Somit ist κ ein Antiautomorphismus von $L_{S,V}$.

Es seien nun X und Y zwei verschiedene Punkte von $L_{S,V}$, die in L auf einer Geraden durch S liegen. Wäre nun $Z := X^\kappa \cap Y^\kappa$ ein Punkt von $L_{S,V}$, so wäre Z^λ eine Gerade von $L_{S,V}$ mit $X, Y \leq Z^\lambda$. Es folgte der Widerspruch $S \leq X + Y = Z^\lambda$. Dies impliziert, dass die Punkte einer Geraden durch S von κ auf konfluente Geraden abgebildet werden, deren gemeinsamer Schnittpunkt auf V liegt. Bei diesem Schluss haben wir nur davon Gebrauch gemacht, dass κ ein Antiautomorphismus von $L_{S,V}$ ist und dass $\lambda = \kappa^{-1}$ gilt. Aus Dualitätsgründen bildet λ daher konfluente Geraden, die sich in einem von S verschiedenen Punkt auf V schneiden, auf Punkte ab, die auf einer Geraden durch S liegen. Dies ist nun mehr als genug, um mit I.8.8 zu schließen, dass κ durch eine Korrelation von L induziert wird, die wir ebenfalls κ nennen.

Es sei X ein von S verschiedener Punkt auf G. Dann ist

$$\begin{aligned} X^\kappa &= \big((X+P) \cap G\big) + \big((X+Q) \cap H\big) = X + \big((X+Q) \cap H\big) \\ &= (X+Q) \cap (X+H) = X + Q, \end{aligned}$$

da ja X nicht auf H liegt. Hieraus folgt, dass X ein absoluter Punkt und dass $G^\kappa = Q$ ist. Entsprechend folgt, dass die von S verschiedenen Punkte von H absolut sind und dass $H^\kappa = P$ ist. Also ist $S^\kappa = (G \cap H)^\kappa = Q + P = V$. Somit ist auch S absolut und κ als (G, H)-Korrelation erkannt.

Es sei Z eine von V verschiedene Gerade durch P. Setzt man $X := Z \cap G$ und $Y := Z \cap H$, so ist

$$Z^\kappa = (X+Y)^\kappa = X^\kappa \cap Y^\kappa = (X+Q) \cap (Y+P) = (X \cap Q) \cap Z = X.$$

Hieraus folgt, dass $P^\kappa = G$ ist. Ebenso folgt $Q^\kappa = H$. Damit ist gezeigt, dass 2) eine Folge von 1) ist.

Es bleibe dem Leser überlassen zu zeigen, dass 1) eine Folge von 2) ist.

Nun sind wir endlich in der Lage, den Satz von Hessenberg zu beweisen.

4.4. Satz von Hessenberg. *Jede pappossche Ebene ist desarguessch.*

Beweis. Es sei (P, H) ein nicht inzidentes Punkt-Geradenpaar der papposschen projektiven Ebene L. Ferner sei V eine Gerade durch P. Setze $S := V \cap H$ und G sei eine von V und H verschiedene Gerade durch S. Schließlich seien X und Y zwei Punkte auf V, die von P und S verschieden sind. Nach 4.3 gibt es dann zwei (G, H)-Korrelationen κ und λ mit $P^\kappa = P^\lambda = G$ und $X^\kappa = Y^\lambda = H$. Setze $\sigma := \kappa\lambda^{-1}$. Dann ist $P^\sigma = P$ und $X^\sigma = Y$. Ist Z ein Punkt auf H, so folgt mit 4.2

$$Z^\sigma = Z^{\kappa\sigma^{-1}} = (Z+P)^{\lambda^{-1}} = Z.$$

Folglich ist $\sigma \in \Delta(P, H)$ und L ist als (P, H)-transitiv erkannt. Da dies für alle nicht inzidenten Punkt-Geradenpaare von L gilt, folgt mit 1.11, dass L für alle Punkt-Geradenpaare eine (P, H)-transitive Ebene ist, seien sie inzident oder nicht. Damit ist der Satz von Hessenberg bewiesen.

Ich denke, dass der Leser mit mir einer Meinung ist, dass dieser Beweis des hessenbergschen Satzes ein Juwel ist.

5. Weniger Bekanntes aus der linearen Algebra

Ist V ein Rechtsvektorraum über dem Körper K, so ist $L(V)$ mit der Inklusion als Teilordnung ein projektiver Verband. Ist H eine Hyperebene dieses Verbandes und P ein Punkt, der nicht auf H liegt, so haben wir die Objekte $\Delta(P,H)$, $\mathrm{E}(H)$ und $K(H)$, die wir in den ersten beiden Abschnitten dieses Kapitels definiert haben. Es geht uns nun darum, für diese Objekte eine algebraische Beschreibung zu finden. Es wird sich herausstellen, dass $K(H)$ zu K isomorph ist, — wie könnte es anders sein —, und dass $\mathrm{E}(H)$ als $K(H)$-Vektorraum zum K-Vektorraum H isomorph ist. Das hat nach Früherem dann wieder zur Folge, dass $\Delta(P,H)$, falls der Punkt P nicht auf der Hyperebene H liegt, zur multiplikativen Gruppe K^* isomorph ist.

Wir beginnen mit der Darstellung von $\mathrm{E}(H)$. Kandidaten zur Beschreibung von Elationen sind solche linearen Abbildungen von V in sich, die eine Hyperebene vektorweise festlassen und ebenso den Faktorraum nach dieser Hyperebene. Es wird sich herausstellen, dass sich in der Tat jede Elation durch eine solche lineare Abbildung darstellen lässt.

Es sei V ein Vektorraum über dem Körper K mit $\mathrm{Rg}_K(V) \geq 2$. Ferner sei H eine Hyperebene von V. Ist τ ein Endomorphismus von V, so nennen wir τ *Transvektion* mit der *Achse* H von V, falls τ auf H und V/H die Identität induziert. Mit $\mathrm{T}(H)$ bezeichnen wir die Menge aller Transvektionen mit der Achse H. Offensichtlich ist $\mathrm{T}(H)$ eine multiplikativ abgeschlossene Teilmenge des Endomorphismenringes von V, die die Identität enthält. Es sei $\tau \in \mathrm{T}(H)$. Dann gilt zunächst

$$v^\tau = v + v^\tau - v$$

für alle $v \in V$. Weil τ auf V/H die Identität induziert, folgt $v^\tau - v \in H$. Wir definieren τ' durch

$$v^{\tau'} := v - v^\tau + v.$$

Es folgt $\tau' \in \mathrm{T}(H)$ und $\tau\tau' = 1 = \tau'\tau$, wie eine einfache Rechnung bestätigt. Dies besagt, dass $\mathrm{T}(H)$ sogar eine Untergruppe der Einheitengruppe des Endomorphismenringes von V ist.

Ist $\tau \in \mathrm{T}(H)$, so induziert τ in $L(V)$ natürlich eine Perspektivität mit der Achse H. Lässt τ einen Punkt außerhalb von H invariant, so induziert τ auf diesem Punkt die Identität, ist also selbst die Identität. Folglich induziert jede Transvektion mit der Achse H eine Elation mit der Achse H in $L(V)$. Mehr noch: Die Gruppe $\mathrm{T}(H)$ ist isomorph zu einer Untergruppe von $\mathrm{E}(H)$, da ja nur die Identität aus $\mathrm{T}(H)$ Fixpunkte außerhalb H hat. Dies impliziert, dass $\mathrm{T}(H)$ abelsch ist. Wir werden gleich sehen, dass jede Elation durch eine Transvektion induziert wird.

Ginge man nun didaktisch geschickt vor, um das Folgende zu motivieren, so käme man bald in technische Schwierigkeiten, so dass man nach der Motivation noch einmal von vorne beginnen müsste. Dies zeigten mir jedenfalls meine Versuche. Da ich aber weiß, wie es weitergeht, spare ich mir die Motivation und dem Leser das Lesen meiner Schmierzettel.

5.1. Satz. *Es sei V ein Rechtsvektorraum über dem Körper K mit $\mathrm{Rg}_K(V) \geq 2$. Ferner sei P ein Punkt und H eine Hyperebene von $L(V)$ mit $V = P \oplus H$. Schließlich sei $P = pK$. Wir definieren die Abbildung φ von V in K durch*

$$\varphi(pk + h) := k$$

für alle $k \in K$ und alle $h \in H$. Dann ist $\varphi \in V^*$ und $H = \mathrm{Kern}(\varphi)$. Für $h \in H$ definieren wir die Abbildung $\tau(h)$ durch

$$v^{\tau(h)} := v + h\varphi(v)$$

für alle $v \in V$. Dann ist τ ein Isomorphismus der Gruppe H auf die Gruppe $\mathrm{T}(H)$ aller Transvektionen mit der Achse H.

Ist $\mathrm{Rg}_K(V) \geq 3$, so wird $\mathrm{E}(H)$ von $\tau(H)$ treu induziert. Ist $0 \neq h \in H$, so ist hK das Zentrum der von $\tau(h)$ induzierten Elation.

Beweis. Es ist banal nachzurechnen, dass $\varphi \in V^*$ und $\mathrm{Kern}(\varphi) = H$ ist. Weil φ linear ist, ist auch $\tau(h)$ linear, so dass $\tau(h)$ ein Endomorphismus von V ist. Da $\tau(h)$ offensichtlich auf H und V/H die Identität induziert, gilt $\tau(h) \in \mathrm{T}(H)$. Weiter gilt

$$\begin{aligned} v^{\tau(h)\tau(h')} &= \big(v + h\varphi(v)\big)^{\tau(h')} \\ &= v^{\tau(h')} + h^{\tau(h')}\varphi(v) \\ &= v + h'\varphi(v) + h\varphi(v) \\ &= v + (h + h')\varphi(v) \\ &= v^{\tau(h+h')}, \end{aligned}$$

so dass $\tau(h+h') = \tau(h)\tau(h')$ ist. Schließlich folgen aus $\tau(h) = 1$ die Gleichungen

$$p = p^{\tau(h)} = p + h$$

und damit $h = 0$. Dies zeigt, dass τ ein Monomorphismus von H in $\mathrm{T}(H)$ ist.

Wir müssen noch zeigen, dass τ sogar surjektiv ist. Dazu sei Q ein von P verschiedenes Komplement von H und $C := (P+Q) \cap H$. Dann ist C ein Punkt auf H, so dass $P + Q = Q + C$ ist. Es gibt also ein $q \in Q$ und ein $c \in C$, so dass $p = q - c$ ist. Es folgt

$$p^{\tau(c)} = p + c\varphi(p) = p + c = q.$$

Weil p nicht Null ist, ist auch q nicht Null. Folglich ist $P^{\tau(c)} = Q$. Somit ist $\tau(H)$ — dies ist kein Druckfehler — auf der Menge der Punkte, die nicht auf H liegen, transitiv. Weil die einzige Abbildung in $\mathrm{T}(H)$, die einen Punkt außerhalb H festlässt, die Identität ist, folgt hieraus, dass $\tau(H) = \mathrm{T}(H)$ ist.

Es sei schließlich $0 \neq h \in H$ und X sei ein Teilraum von V, der hK enthält. Ist dann $y \in X$, so ist

$$y^{\tau(h)} = y + h\varphi(y) \in X,$$

so dass $X^{\tau(h)} = X$ ist. Damit ist alles bewiesen.

Man beachte, dass der Isomorphismus τ von der Wahl von p abhängt.

Es sei wieder V ein Vektorraum über dem Körper K. Ferner sei P ein Punkt und H eine Hyperebene von V mit $V = P \oplus H$. Ist σ ein Endomorphismus von V, der auf H die Identität induziert, und der weiterhin $P^\sigma = P$ erfüllt, so heißt σ *Homothetie* mit dem *Zentrum* P und der *Achse* H von V. Die Homothetien mit dem Zentrum P und der Achse H bilden eine Untergruppe der Einheitengruppe des Endomorphismenringes von V, die wir mit $\Sigma(P, H)$ bezeichnen.

Es sei $\lambda \in \Sigma(P, H)$. Ist $0 \neq p \in P$, so gibt es genau ein $a \in K^*$ mit $p^\lambda = pa$. Hieraus folgt

$$(pk + h)^\lambda = p^\lambda k + h^\lambda = pak + h$$

für alle $k \in K$ und alle $h \in H$. Homothetien lassen sich also sehr einfach beschreiben. Diese Beschreibung wird nun im nächsten Satz zur Definition benutzt. Dabei sei für den Leser, der eine der weniger guten Vorlesungen über lineare Algebra gehört hat — alle betrachteten Körper seien kommutativ —, hier ausdrücklich bemerkt, dass der Koeffizient a zwischen p und k stehen muss, da nur so die Linearität der gleich zu definierenden Abbildung $\delta(a)$ erzwungen wird.

5.2. Satz. *Es sei V ein Vektorraum über dem Körper K und es gelte* $\mathrm{Rg}_K(V) \geq 2$. *Ferner seien P ein Punkt und H eine Hyperebene von $L(V)$ mit $V = P \oplus H$. Schließlich sei $0 \neq p \in P$. Für $a \in K^*$ definieren wir die Abbildung $\delta(a)$ von V in sich durch*

$$(pk + h)^{\delta(a)} := pa^{-1}k + h$$

für alle $k \in K$ und alle $h \in H$. Dann ist δ ein Isomorphismus von K^* auf $\Delta(P, H)$.

Ist $\mathrm{Rg}_K(V) \geq 3$, *so wird $\Delta(P, H)$ von $\Sigma(P, H)$ treu induziert.*

Beweis. Eine banale Rechnung zeigt, dass $\delta(a)$ linear ist. Hieraus folgt dann, dass $\delta(a) \in \Sigma(P, H)$ gilt.

Es sei $0 \neq a$, $b \in K^*$. Dann ist

$$\begin{aligned}(pk + h)^{\delta(ab)} &= p(ab)^{-1}k + h \\ &= pb^{-1}a^{-1}k + h \\ &= p^{\delta(b)}a^{-1}k + h^{\delta(b)} \\ &= (pa^{-1}k + h)^{\delta(b)} \\ &= (pk + h)^{\delta(a)\delta(b)},\end{aligned}$$

so dass $\delta(ab) = \delta(a)\delta(b)$ ist. Folglich ist δ ein Homomorphismus.

Um die Injektivität zu beweisen, beweisen wir etwas mehr, nämlich, dass $\delta(a)$ genau dann einen von P verschiedenen Punkt Q von $L(V)_H$ festlässt, wenn $a = 1$ ist. Es sei also Q ein solcher Punkt und es gelte $Q^{\delta(a)} = Q$. Weil $P + Q$ eine Gerade ist, ist $C := (P + Q) \cap H$ ein Punkt, der überdies von P und Q verschieden ist. Es gibt daher von 0 verschiedene Vektoren p', q' und c' mit $p' \in P$, $q' \in Q$ und $c' \in C$ und $q' = p' + c'$. Es gibt ferner ein von 0 verschiedenes $k \in K$ mit $p = p'k$. Setze $q := q'k$ und $c := c'k$. Dann sind auch p, q und c

von 0 verschieden und es gilt $q = p + c$. Wegen $Q^{\delta(a)} = Q$ gibt es ein $l \in K$ mit $q^{\delta(a)} = ql$. Es folgt

$$pl + cl = q^{\delta(a)} = (p + c)^{\delta(a)} = pa^{-1} + c.$$

Weil p und c linear unabhängig sind, folgt hieraus $a^{-1} = l = 1$, so dass $a = 1$ ist, und zum Andern, dass $\Sigma(P, H)$ eine Untergruppe von $\Delta(P, H)$ treu induziert, falls nur $\mathrm{Rg}_K(V) \geq 3$ ist, da nur in diesem Falle $\Delta(P, H)$ definiert ist.

Ist $\lambda \in \Sigma(P, H)$, so haben wir schon gesehen, dass es ein $a \in K^*$ gibt mit $\delta(a^{-1}) = \lambda$. Somit ist δ auch surjektiv.

Es sei $\mathrm{Rg}_K(V) \geq 3$. In diesem Falle müssen wir noch zeigen, dass $\Sigma(P, H)$ alle Kollineationen in $\Delta(P, H)$ induziert. Zu diesem Zweck seien P_1 und P_2 zwei von P verschiedene Komplemente von H mit $P + P_1 = P + P_2$. Setze $C := (P + P_1) \cap H$. Dann ist C ein Punkt auf H. Es gibt also wieder von 0 verschiedene $p_i \in P_i$ und c_1, $c_2 \in C$ mit $p_i = p + c_i$ für $i := 1, 2$. Es gibt ferner ein $a \in K^*$ mit $c_2 = c_1 a$. Damit folgt nun

$$p_1^{\delta(a)} = pa^{-1} + c_1 = (p + c_2)a^{-1} = p_2 a^{-1}.$$

Also ist $P_1^{\delta(a)} = P_2$. Dies beweist nach nun schon sattsam bekannten Sätzen auch die noch offene letzte Behauptung des Satzes.

Auf Grund der beiden Sätze 5.1 und 5.2 dürfen wir im folgenden die Gruppe $\mathrm{T}(H)$ mit $\mathrm{E}(H)$ und die Gruppe $\Sigma(P, H)$ mit $\Delta(P, H)$ identifizieren.

5.3. Satz. *Es sei V ein Vektorraum über dem Körper K und es gelte* $\mathrm{Rg}_K(V) \geq 3$. *Ferner sei P ein Punkt und H eine Hyperebene von $L(V)$ mit $V = P \oplus H$. Wir definieren eine Abbildung δ^* von K in den Endomorphismenring von* $\mathrm{E}(H)$ *durch* $\delta^*(0) := 0$ *und*

$$\rho^{\delta^*(a)} := \delta(a)^{-1} \rho \delta(a)$$

für alle $\rho \in \mathrm{E}(H)$ und alle $a \in K^*$. Dann ist $\tau(h)^{\delta^*(a)} = \tau(ha)$ für alle $h \in H$ und alle $a \in K$. Insbesondere ist (τ, δ^*) ein Isomorphismus des K-Vektorraumes H auf den $K(H)$-Vektorraum $\mathrm{E}(H)$.

Bevor wir mit dem Beweise des Satzes beginnen, scheint noch ein Wort des Kommentars angebracht. Auch gute Vorlesungen über lineare Algebra kommen meist nicht auf den Begriff der semilinearen Abbildung zu sprechen. In der Geometrie ist man aber durch die Sache gezwungen, auch von diesen zu reden, wie sich hier zum ersten Male zeigt. Es ist also an der Zeit den Begriff der semilinearen Abbildung zu definieren. Dazu sei V ein Vektorraum über K und V' ein solcher über K'. Ist dann σ ein Homomorphismus der abelschen Gruppe V in die abelsche Gruppe V', ist α ein Isomorphismus des Körpers K auf den Körper K' und gilt

$$(vk)^\sigma = v^\sigma k^\sigma$$

für alle $v \in V$ und alle $k \in K$, so heißt das Paar (σ, α) *semilineare Abbildung* von V in V'. Es bedarf nun nicht mehr viel an Fantasie, um den Begriff des Isomorphismus von Vektorräumen zu definieren.

Beweis. Mit 2.1 folgt, dass δ^* eine surjektive Abbildung von K auf $K(H)$ ist. Ferner ist klar, dass $\tau(h)^{\delta^*(0)} = \tau(h0)$ ist. Es sei also $a \in K^*$. Zu $h \in H$ gibt es dann ein $h' \in H$ mit $\tau(h)^{\delta^*(a)} = \tau(h')$. Um $\tau(h')$ zu bestimmen, genügt es, die Wirkung von $\tau(h')$ auf den Punkt P zu bestimmen. Wegen $\varphi(p) = 1$ ist nun

$$\begin{aligned} p + h' &= p^{\tau(h')} = p^{\delta(a)^{-1}\tau(h)\delta(a)} \\ &= \big(pa + h\varphi(pa)\big)^{\delta(a)} = p + ha. \end{aligned}$$

Somit ist $h' = ha$, so dass $\tau(h)^{\delta^*(a)} = \tau(ha)$ ist. Routinerechnungen zeigen nun, dass δ^* ein Homomorphismus von K auf $K(H)$ ist. Weil nicht triviale Homomorphismen von Körpern stets Monomorphismen sind, ist bereits alles bewiesen.

6. Der erste Struktursatz

In diesem Abschnitt werden wir den schon angekündigten Satz beweisen, dass sich jeder desarguessche projektive Verband als Unterraumverband eines Vektorraumes darstellen lässt. Eine unmittelbare Folgerung aus ihm wird der von Hilbert stammende Satz sein, dass eine desarguessche projektive Geometrie genau dann papposch ist, wenn der zu Grunde liegende Koordinatenkörper kommutativ ist (Hilbert 1899). Damit werden wir zusammen mit dem hessenbergschen Satz eine befriedigende Beschreibung aller papposschen Geometrien erhalten.

6.1. Erster Struktursatz. *Ist L ein irreduzibler projektiver Verband vom Rang* $\mathrm{Rg}(L) \geq 3$ *und ist L in Falle* $\mathrm{Rg}(L) = 3$ *desarguessch, so gibt es einen und bis auf Isomorphie auch nur einen Vektorraum V über einem Körper K, so dass L und $L(V)$ isomorph sind.*

Beweis. Wir beweisen zuerst die Eindeutigkeitsaussage. Es seien L und L' zwei desarguessche projektive Verbände und σ sei ein Isomorphismus von L auf L'. Ferner sei H eine Hyperebene von L und $H' := H^\sigma$. Ist $\tau \in \mathrm{E}(H)$ und $\kappa \in K(H)$, so setzen wir $\tau^{\sigma^*} := \sigma^{-1}\tau\sigma$ und $\kappa^{\sigma^{**}} := (\sigma^*)^{-1}\kappa\sigma^*$. Eine simple Rechnung zeigt, dass das so definierte Abbildungspaar ein Isomorphismus des $K(H)$-Vektorraumes $\mathrm{E}(H)$ auf den $K(H')$-Vektorraum $\mathrm{E}(H')$ ist. Ist nun $L = L(V)$ und $L' = L(V')$, so folgt aus dieser Bemerkung, aus $\mathrm{Rg}_K(V) = \mathrm{Rg}(L) = \mathrm{Rg}(L') = \mathrm{Rg}_{K'}(V')$ und aus 5.3 sowie aus dem Struktursatz für Vektorräume, dass nämlich ein Vektorraum über dem Körper K durch seinen Rang und eben diesen Körper bis auf Isomorphie eindeutig bestimmt ist, dass V und V' isomorph sind.

Den Beweis der Existenzaussage beginnen wir mit einer Vorbemerkung. Es sei L ein desarguesscher projektiver Verband und H sei eine Hyperebene von L. Die Gruppe $\mathrm{E}(H)$ operiert dann scharf transitiv auf der Menge der Punkte von L_H. Ist O ein Punkt von L_H, so gibt es zu jedem Punkt P von L_H genau ein $\tau_P \in \mathrm{E}(H)$ mit

$$O^{\tau_P} = P.$$

Die Abbildung τ ist eine Bijektion der Punktmenge von L_H auf $\mathrm{E}(H)$. Ist nun $X \leq H$, so gilt offensichtlich $P \leq O + X$ genau dann, wenn $\tau_P \in \mathrm{E}(X)$ ist. Bezeichnet Π wieder das größte Element von L, so folgt mittels Satz 2.4, dass τ einen Isomorphismus von Π/O auf den Verband der Unterräume des $K(H)$-Vektorraumes $\mathrm{E}(H)$ induziert. Hieraus folgt schließlich auf Grund der Transitivität von $E(H)$, dass τ einen Isomorphismus von L_H auf den Verband der Rechtsrestklassen nach allen Unterräumen von $\mathrm{E}(H)$ induziert. (Hieran könnte man nun didaktische Bemerkungen über freie Vektoren, den Elementen von $\mathrm{E}(H)$, und Ortsvektoren, der Beschreibung der Punktmenge von L_H mittels O und τ, anschließen. Diese niemals sauber definierten Begriffe sind eine ständig fließende Quelle der Konfusion. Der Leser wird jedoch genügend Fantasie besitzen, anhand der vorstehenden Bemerkungen eine Trennung der beiden Begriffe vornehmen zu können, so dass sich weitere Bemerkungen meinerseits erübrigen. Sie würden den richtigen Adressaten ja doch nicht erreichen.)

Mit Hilfe der Vorbemerkung ist es nun ein Leichtes, die Existenzaussage des Satzes zu beweisen. Es sei also L ein desarguesscher projektiver Verband und H sei eine Hyperebene von L. Ferner sei V ein Vektorraum über $K(H)$ mit $\mathrm{Rg}_{K(H)}(V) = \mathrm{Rg}(L)$. Einen solchen Vektorraum gibt es stets. (Um dies einzusehen, betrachte man die Menge aller Abbildungen einer Basis von L in $K(H)$ mit endlichem Träger. Diese Menge versehen mit der punktweise definierten Addition und Skalarmultiplikation ist ein solcher.) Es sei weiter H' eine Hyperebene von V. Nach 5.3 sind $K(H')$ und $K(H)$ isomorph. Mittels 2.4 und $\mathrm{Rg}_{K(H)}(V) = \mathrm{Rg}(L)$ folgt

$$\mathrm{Rg}_{K(H)}(\mathrm{E}(H)) = \mathrm{Rg}_{\Pi}(H) = \mathrm{Rg}_{\Pi'}(H') = \mathrm{Rg}_{K(H')}\big(\mathrm{E}(H')\big).$$

Hieraus folgt weiter, dass der $K(H)$-Vektorraum $\mathrm{E}(H)$ zu dem $K(H')$-Vektorraum $\mathrm{E}(H')$ isomorph ist. Unsere Vorbemerkung sagt dann aber, dass auch L_H und $L(V)_{H'}$ isomorph sind. Hieraus folgt schließlich mittels I.8.8, dass auch L und $L(V)$ isomorph sind. Damit ist alles bewiesen.

Wie der Beweis zeigt, gilt auch der folgende, von André stammende Satz (André 1954).

6.2. Satz. *Ist L eine Translationsebene bezüglich der Geraden H, so ist L genau dann desarguessch, wenn der $K(H)$-Vektorraum $\mathrm{E}(H)$ den Rang 2 hat.*

Ist L ein desarguesscher projektiver Verband, so gibt es also einen Vektorraum V über einem Körper K mit $L \cong L(V)$. Man nennt V den L *zu Grunde liegenden Vektorraum* und K den *Koordinatenkörper* von L. Mit 3.1 und 3.5 folgt daher der schon angekündigte Satz von Hilbert (Hilbert 1899).

6.3. Satz. *Ein desarguesscher projektiver Verband ist genau dann papposch, wenn sein Koordinatenkörper kommutativ ist.*

Da es Körper gibt, die nicht kommutativ sind, gibt es auch projektive Räume, in denen der Satz von Pappos nicht gilt. Beispiele solcher Körper werden wir später noch kennenlernen.

Ist q Potenz einer Primzahl, so gibt es einen und bis auf Isomorphie auch nur einen Körper mit q Elementen, nämlich das Galoisfeld $\mathrm{GF}(q)$. Daher gilt auch das

6.4. Korollar. *Ist q Potenz einer Primzahl und ist n eine natürliche Zahl mit $n \geq 4$, so gibt es einen und bis auf Isomorphie auch nur einen endlichen irreduziblen projektiven Verband der Ordnung q und des Ranges n.*

Dieser Satz ist für $n = 3$ falsch, da es nicht desarguessche projektive Ebenen gibt.

7. Der zweite Struktursatz

Sind V und V' Vektorräume über K und K', so induziert jeder Isomorphismus von V auf V' einen Isomorphismus von $L(V)$ auf $L(V')$. Die Umkehrung dieses Sachverhaltes ist Inhalt des zweiten Struktursatzes, den wir jetzt formulieren und beweisen werden. Dabei sei daran erinnert, dass Isomorphismen von Vektorräumen auch semilinear sein können.

7.1. Zweiter Struktursatz. *Sind V und V' zwei Vektorräume über K bzw. K', ist $\mathrm{Rg}_K(V) \geq 3$ und ist σ ein Isomorphismus von $L(V)$ auf $L(V')$, so wird σ durch einen Isomorphismus von V auf V' induziert.*

Beweis. Aus dem ersten Struktursatz folgt, dass V und V' isomorph sind, so dass wir annehmen dürfen, dass $V = V'$ und $K = K'$ ist. Satz 5.1 lehrt, dass alle Elationen von $L(V)$ sogar durch lineare Automorphismen von V induziert werden, und die Gruppe von Kollineationen, die von allen Elationen erzeugt wird, ist nach 3.2 auf der Menge der nicht inzidenten Punkt-Hyperebenenpaare von $L(V)$ transitiv. Wir dürfen daher des Weiteren annehmen, dass es ein nicht inzidentes Punkt-Hyperebenenpaar (P, H) gibt mit $P^\sigma = P$ und $H^\sigma = H$. Dann ist

$$\sigma^{-1}\mathrm{E}(H)\sigma = \mathrm{E}(H^\sigma) = \mathrm{E}(H),$$

so dass der durch σ induzierte Automorphismus der Kollineationsgruppe von $L(V)$ einen Automorphismus auf $\mathrm{E}(H)$ induziert. Wir definieren die Abbildung σ^* durch

$$\tau(h^{\sigma^*}) := \sigma^{-1}\tau(h)\sigma.$$

Mit 5.1 folgt, dass σ^* ein Automorphismus der abelschen Gruppe H ist.

Es sei $a \in K$. Ist $a = 0$, so ist $\tau((ha)^{\sigma^*}) = 1 = \tau(h^{\sigma^*}a)$. Es sei also $a \neq 0$. Nach 5.3 ist dann

$$\begin{aligned}\tau\big((ha)^{\sigma^*}\big) &= \sigma^{-1}\tau(ha)\sigma \\ &= \sigma^{-1}\delta(a)^{-1}\sigma\sigma^{-1}\tau(h)\sigma\sigma^{-1}\delta(a)\sigma \\ &= \sigma^{-1}\delta(a)^{-1}\sigma\tau(h^{\sigma^*})\sigma^{-1}\delta(a)\sigma.\end{aligned}$$

Nun ist

$$\sigma^{-1}\Delta(P, H)\sigma = \Delta(P^\sigma, H^\sigma) = \Delta(P, H).$$

Also induziert σ einen Automorphismus in $\Delta(P,H)$. Es gibt daher zu jedem $a \in K^*$ ein $a^{\sigma^{**}} \in K^*$ mit

$$\sigma^{-1}\delta(a)\sigma = \delta(a^{\sigma^{**}}).$$

Setzt man noch $0^{\sigma^{**}} := 0$, so ist σ^{**} eine Bijektion von K auf sich und es gilt

$$\tau\big((ha)^{\sigma^*}\big) = \tau(h^{\sigma^*}a^{\sigma^{**}})$$

für alle $h \in H$ und alle $a \in K$. Hieraus folgt wiederum, da τ injektiv ist, dass

$$(ha)^{\sigma^*} = h^{\sigma^*}a^{\sigma^{**}}$$

für alle $h \in H$ und alle $k \in K$ gilt. Routinerechnungen zeigen nun, dass (σ^*, σ^{**}) ein Automorphismus des $K(H)$-Vektorraumes H ist.

Es sei $0 \neq p \in P$. Dann ist $V = pK \oplus H$. Wir definieren die Abbildung ρ^* von V in sich durch

$$(pa + h)^{\rho^*} := pa^{\sigma^{**}} + h^{\sigma^*}.$$

Dann ist (ρ^*, σ^{**}) ein Automorphismus von V. Nun ist $p^{\sigma^*} = p$ und daher

$$\begin{aligned} p^{\rho^{*-1}\tau(h)\rho^*} &= p^{\tau(h)\rho^*} \\ &= (p+h)^{\rho^*} \\ &= p^{\tau(h^{\sigma^*})}. \end{aligned}$$

Also ist $\rho^{*-1}\tau(h)\rho^* = \tau(h^{\sigma^*})$. Ist ρ die von ρ^* in $L(V)$ induzierte Kollineation, so ist also $\rho^{-1}\tau(h)\rho = \sigma^{-1}\tau(h)\sigma$. Daher ist $\sigma\tau^{-1}$ für alle $h \in H$ mit $\tau(h)$ vertauschbar. Nun ist $P^{\sigma\rho^{-1}} = P$ und folglich

$$P^{\tau(h)} = P^{\sigma\rho^{-1}\tau(h)} = (P^{\tau(h)})^{\sigma\rho^{-1}}$$

für alle $h \in H$. Weil $\mathrm{E}(H)$ auf der Menge der Punkte von $L(V)_H$ transitiv operiert, folgt, dass $\sigma\rho^{-1}$ alle Punkte von $L(V_H)$ zu Fixpunkten hat, so dass nach I.8.8 die Gleichung $\sigma\rho^{-1} = 1$ gilt. Folglich ist $\sigma = \rho$, was wir zu beweisen hofften.

8. Der dritte Struktursatz

Der erste in diesem Abschnitt zu beweisende Satz verdient eigentlich auch den Namen Struktursatz. Er lautet:

8.1. Satz. *Ist L ein desarguesscher projektiver Verband, so ist L genau dann selbstdual, wenn der Rang von L endlich ist und der L zu Grunde liegende Koordinatenkörper einen Antiautomorphismus besitzt.*

Beweis. Es sei K der L zu Grunde liegende Koordinatenkörper.

Ist L selbstdual, so folgt mit I.5.7, dass der Rang von L endlich ist. Die nach I.5.19 gemachte Bemerkung zeigt, dass $K_\circ$ der Koordinatenkörper von L^d ist. Weil L zu L^d isomorph ist, folgt aus dem ersten Struktursatz, dass es einen

Isomorphismus α von K auf $K_\circ$ gibt. Dann ist α aber nichts Anderes als ein Antiautomorphismus von K.

Es sei umgekehrt der Rang von L endlich und α sei ein Antiautomorphismus von K. Dann ist α ein Isomorphismus von K auf $K_\circ$. Ist V der L zu Grunde liegende Vektorraum, so ist der $K_\circ$-Vektorraum V^* der L^d zu Grunde liegende Vektorraum. Da nach I.5.17 die Ränge von V und V^* gleich sind, ist der K-Vektorraum V zum $K_\circ$-Vektorraum V^* isomorph. Folglich sind auch L und L^d isomorph, so dass L selbstdual ist.

Da bei einem kommutativen Körper die Identität stets auch ein Antiautomorphismus ist, gilt, wie schon in Abschnitt 5 des ersten Kapitels, wenn auch in etwas anderer Formulierung, bemerkt, das

8.2. Korollar. *Ein papposscher projektiver Raum endlichen Ranges ist stets selbstdual. Insbesondere sind alle endlichen desarguesschen projektiven Räume selbstdual.*

Es gibt Körper, die keinen Antiautomorphismus gestatten. Ist nämlich K ein Körper des Ranges $n < \infty$ über seinem Zentrum, so zeigt die Theorie der einfachen Algebren, dass K höchstens dann einen Antiautomorphismus besitzt, wenn n eine Potenz von 2 ist (siehe etwa Deuring 1968, Satz 11, S. 45 und Satz 2, S. 59).

Es sei f eine Abbildung von $V \times V$ in K und α sei ein Antiautomorphismus von K. Die Abbildung f heißt α-*Semibilinearform*, falls gilt:

a) Es ist $f(u+v,w) = f(u,w) + f(v,w)$ und $f(u,v+w) = f(u,v) + f(u,w)$ für alle u, v, $w \in V$.

b) Es ist $f(uk,v) = k^\alpha f(u,v)$ und $f(u,vk) = f(u,v)k$ für alle u, $v \in V$ und alle $k \in K$.

Ist κ eine Korrelation von $L(V)$, so sagen wir, dass κ durch die α-Semibilinearform f *dargestellt* werde, falls

$$U^\kappa = \big\{v \mid v \in V, f(u,v) = 0 \text{ für alle } u \in U\big\}$$

für alle $U \in L(V)$ ist. Es gilt nun:

8.3. Dritter Struktursatz. *Es sei V ein Vektorraum über dem Körper K mit* $\mathrm{Rg}_K(V) \geq 3$. *Ist κ eine Korrelation von $L(V)$, so wird κ durch eine α-Semibilinearform dargestellt.*

Beweis. Es sei W der Dualraum zu V. Beide Räume haben dann nach 8.1 den gleichen, endlichen Rang. Für $X \in L(V)$ setzen wir

$$X^\pi := \big\{w \mid w \in W,\ wX = \{0\}\big\}.$$

Dies ist die Abbildung, die wir im fünften Abschnitt des ersten Kapitels mit $\perp$ bezeichneten. Nach I.5.19 ist π ein Isomorphismus von $L(V)^d$ auf $L(W)$, so dass $\kappa\pi$ ein Isomorphismus von $L(V)$ auf $L(W)$ ist. Nach dem zweiten Struktursatz

gibt es also einen Isomorphismus (ρ, α) des K-Vektorraumes V auf den $K_\circ$-Vektorraum W mit $X^\rho = X^{\kappa\pi}$ für alle $X \in L(V)$. Weil α ein Isomorphismus von K auf $K_\circ$ ist, ist α ein Antiautomorphismus von K. Ferner gilt

$$(vk)^\rho = v^\rho \circ k^\alpha = k^\alpha v^\rho$$

für alle $v \in V$ und alle $k \in K$. Wir definieren nun f durch

$$f(u, v) := u^\rho v$$

für alle u, $v \in V$. Triviale Rechnungen zeigen, dass f eine α-Semibilinearform ist.

Es sei $U \in L(V)$. Dann ist $U^{\kappa\pi} = U^\rho$. Ist $v \in U^\kappa$ und $u \in U$, so ist $u^\rho \in U^{\kappa\pi}$ und daher $f(u, v) = u^\rho v = 0$. Ist umgekehrt $u^\rho v = f(u, v) = 0$ für alle $u \in U$, so ist $v \in U^{\rho\pi^{-1}} = U^\kappa$. Also ist

$$U^\kappa = \{v \mid v \in V, f(u, v) = 0 \text{ für alle } u \in U\},$$

was zu beweisen war.

Nicht alle Semibilinearformen stellen Korrelationen dar und verschiedene Semibilinearformen können durchaus auch ein und dieselbe Korrelation darstellen.

Eine α-Semibilinearform f heiße *nicht ausgeartet* oder *nicht entartet*, falls aus der Gültigkeit von $f(u, v) = 0$ für alle $u \in V$ folgt, dass $v = 0$ ist.

8.4. Satz. *Es sei V ein K-Vektorraum mit $3 \leq \mathrm{Rg}_K(V) < \infty$. Die α-Semibilinearform f auf V induziert genau dann eine Korrelation auf $L(V)$, wenn f nicht ausgeartet ist.*

Beweis. Die Korrelation κ werde von f induziert. Aus $V^\kappa = \{0\}$ folgt, dass f nicht ausgeartet ist.

Es sei nun f nicht ausgeartet. Mit W bezeichnen wir den Dualraum von V aufgefasst als Rechtsvektorraum über $K_\circ$. Wir definieren eine Abbildung φ von V in W durch

$$v^\varphi x := f(x, v)^{\alpha^{-1}}$$

für alle v, $x \in V$. Weil α ein Antiautomorphismus ist, ist auch α^{-1} ein solcher. Dies hat zur Folge, dass in der Tat $v^\varphi \in W$ ist. Man verifiziert darüber hinaus mühelos, dass (φ, α^{-1}) eine semilineare Abbildung von V in W ist. Weil f nicht ausgeartet ist, ist φ injektiv. Mittels der Endlichkeit des Ranges von V erschließen wir hieraus, dass (φ, α^{-1}) sogar ein Isomorphismus von V auf W ist.

Wir definieren eine Abbildung κ von $L(V)$ in sich durch

$$U^\kappa := \{v \mid v \in V, f(u, v) = 0 \text{ für alle } u \in U\}.$$

Es sei $X^\kappa = Y^\kappa$. Ist $y \in Y$, jedoch $y \notin X$, so gibt es ein $g \in W$ mit $X \subseteq \mathrm{Kern}(g)$ und $gy = 1$. Nach unserer Vorbemerkung gibt es ein $v \in V$ mit $g = v^\varphi$. Daher ist

$$0 = gx = v^\varphi x = f(x, v)^{\alpha^{-1}}$$

für alle $x \in X$. Hieraus folgt, dass $f(x,v) = 0$ ist für alle $x \in X$. Somit ist $v \in X^\kappa = y^\kappa$ und daher $f(y,v) = 0$. Andererseits ist $1 = (gy)^\alpha = f(y,v)$. Dieser Widerspruch zeigt, dass $Y \leq X$ ist. Ebenso folgt $X \leq Y$, so dass κ als injektiv erkannt ist.

Es ist klar, dass $Y^\kappa \leq X^\kappa$ von $X \leq Y$ impliziert wird. Es sei nun $Y^\kappa \leq X^\kappa$. Es ist $Y \leq X + Y$ und daher $(X+Y)^\kappa \leq Y^\kappa$. Ist $u \in Y^\kappa$, so ist $f(x,u) = 0$ für alle $x \in X$, da ja $Y^\kappa \leq X^\kappa$ ist. Trivialerweise gilt auch $f(y,u) = 0$ für alle $y \in Y$. Daher gilt $f(x+y,u) = 0$ für alle $x \in X$ und alle $y \in Y$. Somit ist $u \in (X+Y)^\kappa$. Damit haben wir auch $Y^\kappa \leq (X+Y)^\kappa$. Also ist $Y^\kappa = (X+Y)^\kappa$. Weil κ injektiv ist, folgt weiter $Y = X + Y$ und damit $X \leq Y$. Folglich gilt $X \leq Y$ genau dann, wenn $Y^\kappa \leq X^\kappa$ ist.

Es sei $b_1, \ldots, b_n$ eine Basis von V. Ferner sei $u = \sum_{i:=1}^n b_i u_i$ und $v = \sum_{i:=1}^n b_i v_i$. Dann ist

$$f(u,v) = \sum_{i:=1}^n u_i^\alpha \sum_{j:=1}^n f(b_i,b_j)v_j.$$

Genau dann ist $f(u,v) = 0$ für alle $u \in V$, wenn

$$\sum_{j:=1}^n f(b_i,b_j)v_j = 0$$

ist für $i := 1, \ldots, n$. Da f nicht ausgeartet ist, hat dieses System linearer Gleichungen nur die triviale Lösung. Daher ist der Rechtsspaltenrang der Matrix $(f(b_i,b_j))$ gleich n. Hieraus folgt, dass der Linkszeilenrang dieser Matrix auch gleich n ist. Definiere g durch

$$g(u,v) := f(v,u)^{\alpha^{-1}}$$

für alle u, $v \in V$. Dann ist g eine α^{-1}-Semibilinearform auf V. Gilt nun $\sum_{j:=1}^n g(b_i,b_j)v_j = 0$ für alle $i := 1, \ldots, n$, so ist

$$0 = \sum_{j:=1}^n f(b_j,b_i)^{\alpha^{-1}} v_j = \left(\sum_{j:=1}^n v_j^\alpha f(b_i,b_j)\right)^{\alpha^{-1}}$$

für alle i. Weil der Linkszeilenrang der Matrix $(f(b_j,b_i))$ gleich n ist, folgt $v_j = 0$ für alle i. Also ist auch g nicht ausgeartet. Definiere λ durch

$$X^\lambda := i\big\{v \mid v \in V, g(u,v) = 0 \text{ für alle } u \in X\big\}.$$

Dann ist λ aus dem gleichen Grunde wie κ eine die Inklusion umkehrende, injektive Abbildung von $L(V)$ in sich. Ferner gilt $X \leq X^{\kappa\lambda}$ und $X \leq X^{\lambda\kappa}$ für alle $X \in L(V)$. Weil X, $X^{\kappa\lambda}$ und $X^{\lambda\kappa}$ den gleichen Rang haben, dies folgt aus der Injektivität von $\kappa\lambda$ und $\lambda\kappa$, und da dieser Rang endlich ist, folgt $X = X^{\kappa\lambda} = X^{\lambda\kappa}$. Folglich ist κ bijektiv und $\lambda = \kappa^{-1}$.

Der gerade geführte Beweis liefert mehr als im Satz formuliert. Was wir mehr bewiesen haben, formulieren wir in den nächsten beiden Korollaren. — Der Leser beachte, dass in 8.5 die Rollen der beiden Argumente von f gegenüber der Definition des Nicht-ausgeartet-seins vertauscht sind!

8.5. Korollar. *Es sei V ein K-Vektorraum mit $3 \leq \mathrm{Rg}_K(V) < \infty$ und f sei eine α-Semibilinearform auf V. Genau dann ist f nicht ausgeartet, wenn aus der Gültigkeit von $f(u,v) = 0$ für alle $v \in V$ folgt, dass $u = 0$ ist.*

Ferner haben wir gesehen, wie die zu einer Korrelation inverse Korrelation sich darstellen lässt.

8.6. Korollar. *Es sei V ein K-Vektorraum mit $3 \leq \mathrm{Rg}_K(V) < \infty$ und κ sei eine Korrelation von $L(V)$. Wird κ durch die α-Semibilinearform f dargestellt, so wird κ^{-1} durch die α^{-1}-Semibilinearform g dargestellt, die durch $g(u,v) := f(v,u)^{\alpha^{-1}}$ definiert wird.*

Schließlich geben wir noch Antwort auf die Frage, wann zwei Semibilinearformen die gleiche Korrelation darstellen.

8.7. Satz. *Es sei V ein Vektorraum über K mit $3 \leq \mathrm{Rg}_K(V) < \infty$. Ferner sei f eine nicht ausgeartete α-Semibilinearform auf V.*

(a) *Ist $k \in K^*$ und definiert man g durch $g(u,v) := k^{-1}f(u,v)$ für alle u, $v \in V$, so ist g eine nicht ausgeartete β-Semibilinearform, wobei β der durch $x^\beta := k^{-1}x^\alpha k$ definierte Antiautomorphismus von K ist. Überdies induzieren f und g die gleiche Korrelation.*

(b) *Ist g eine nicht ausgeartete β-Semibilinearform auf V und stellen f und g die gleiche Korrelation von $L(V)$ dar, so gibt es ein $k \in K^*$ mit $kg(u,v) = f(u,v)$ für alle u, $v \in V$.*

Beweis. (a) Der Leser verifiziert mühelos, dass g eine β-Semibilinearform ist. Dass f und g die gleiche Korrelation von $L(V)$ darstellen, folgt aus der Bemerkung, dass $f(u,v) = 0$ genau dann gilt, wenn $g(u,v) = 0$ ist.

(b) Wir definieren zwei Abbildungen φ und ψ von V in V^* durch $v^\varphi(x) := f(v,x)$ bzw. $v^\psi(x) := g(v,x)$. Weil f und g nicht ausgeartet sind, sind φ und ψ injektiv. Fasst man V^* als Rechtsvektorraum über $K_\circ$ auf, so ist (ψ, β) eine semilineare Abbildung von V in V^*. Daher sind u^ψ und v^ψ genau dann linear unabhängig, wenn u und v es sind.

Weil f und g die gleiche Korrelation darstellen, gilt

$$\mathrm{Kern}(v^\varphi) = \mathrm{Kern}(v^\psi)$$

für alle $v \in V$. Es gibt also zu jedem $v \in V - \{0\}$ genau ein $l(v) \in K^*$ mit $v^\varphi = l(v)v^\psi$. Sind u, $v \in V - \{0\}$, so ist

$$\begin{aligned} l(u+v)u^\psi + l(u+v)v^\psi &= l(u+v)(u+v)^\psi \\ &= (u+v)^v \\ &= u^\varphi + v^\varphi \\ &= l(u)u^\psi + l(v)v^\psi. \end{aligned}$$

Sind nun u und v linear unabhängig, so sind es auch u^ψ und v^ψ, wie wir bemerkten. In diesem Falle gilt also $l(u) = l(u+v) = l(v)$. Sind u und v linear abhängig, so gibt es wegen $\mathrm{Rg}_K(V) \geq 2$ ein $w \in V$ mit $u, v \in wK$. Nach dem bereits Bewiesenen ist dann $l(u) = l(w) = l(v)$. Es gibt also ein $k \in K^*$ mit $l(u) = k$ für alle $v \in V - \{0\}$. Wegen $0^\varphi = 0 = 0^\psi$ gilt also $v^\varphi = kv^\psi$ für alle $v \in V$. Hieraus folgt schließlich

$$f(u,v) = u^\varphi v = (ku^\psi)v = k(u^\psi v) = kg(u,v)$$

für alle $u, v \in V$, so dass auch (b) bewiesen ist.

Es gibt Körper, die einen Antiautomorphismus besitzen, aber keinen involutorischen solchen; siehe Morandi *et alii* 2005.

9. Quaternionenschiefkörper

Es sei K ein Körper und $Z(K)$ sei sein Zentrum. In diesem Falle bezeichnet man mit $[K : Z(K)]$ den Rang von K als $Z(K)$-Vektorraum. Ist $K \neq Z(K)$, so ist $[K : Z(K)] \geq 4$, wie man weiß oder sich schnell überlegt. Ist $[K : Z(K)] = 4$, so heißt K *Quaternionenschiefkörper*. Diese lassen sich sehr schön geometrisch kennzeichnen, wie wir im nächsten Abschnitt sehen werden. Zunächst wollen wir aber zeigen, dass es Quaternionenschiefkörper in Hülle und Fülle gibt. Hierzu lösen wir eine Serie von Aufgaben aus meinem Algebrabuch (Lüneburg 1973, S. 145ff.). Diese Aufgabenserie hat eine Geschichte, die ich dem Leser nicht vorenthalten will: Sie spielt im akademischen Jahr 1970/71, für unsere immer noch junge Universität[1] das Jahr Eins ihres Bestehens.

Wir waren bei der Diskussion der Diplomprüfungsordnung, die im Übrigen bis heute (WS 1989/90 und Jahre darüber hinaus) nicht abgerissen ist. Eines der studentischen Mitglieder des Fachbereichsrates, Gert Schneider, später zu makabrer Berühmtheit gelangt, verlangte, dass die Präambel in der Prüfungsordnung ersatzlos zu streichen sei. In dieser Präambel stand nämlich, dass es Zweck der Prüfung sei fest zu stellen, ob der Kandidat nach wissenschaftlichen Grundsätzen zu arbeiten gelernt habe. Schneider meinte zur Begründung seines Verlangens, es garantiere ja niemand, dass die Studenten während ihres Studiums auch wirklich die Möglichkeit hätten, dies zu lernen. Dies traf mich zutiefst in meiner Berufsehre. Voller Zorn verfasste ich daraufhin eine Serie von drei Übungsblättern mit eben jenen Aufgaben, wobei ich auf dem ersten Blatt verschiedene Möglichkeiten des wissenschaftlichen Arbeitens erläuterte, darunter die Möglichkeit der Verallgemeinerung bekannter Resultate. Im vorliegenden Falle hatte ich nämlich die fraglichen Resultate für den Spezialfall des Ringes der ganzen Zahlen in der Vorlesung vorgerechnet. Diese Aufgabenreihe war also für die damaligen Studenten eine frühe — nicht die erste — Anleitung zum wissenschaftlichen Arbeiten. Rosemarie Rink und Manfred Dugas, dem mathematischen Publikum durch schöne Arbeiten bekannt, haben damals schon durch die Lösung dieser Aufgaben ihr Talent bewiesen.

Im Folgenden bezeichne ω die Menge der nicht negativen ganzen Zahlen.

[1]Sie ist mittlerweile zur Technischen Universität verkümmert.

Es sei R ein Hauptidealbereich und $Q(R)$ sei sein Quotientenkörper. Wir fassen $Q(R)$ auf als Modul über R. Ist p ein Primelement, so bezeichnen wir mit $Z(p^\infty)$ den Teilmodul des Faktormoduls $Q(R)/R$, der aus allen Elementen der Form

$$\frac{r}{p^n} + R$$

mit $r \in R$ und einer nicht negativen ganzen Zahl n besteht. Die Bezeichnung $Z(p^\infty)$ erinnert an die aus der Theorie der abelschen Gruppen bekannten Prüfergruppen, deren Verallgemeinerungen sie sind. Wir nennen $Z(p^\infty)$ sinngemäß *Prüfermodul zum Primelement p* über R. Ferner setzen wir $R_p := \mathrm{End}_R(Z(p^\infty))$. Diesen Ring werden wir zunächst untersuchen.

9.1. Satz. *Es sei R ein Hauptidealbereich und $Z(p^\infty)$ sei der Prüfermodul zum Primelement p von R. Für $i \in \omega$ setzen wir $U_i := \{a \mid a \in Z(p^\infty),\, p^i a = 0\}$. Dann gilt:*

a) *Es ist $U_i \subseteq U_{i+1}$ für alle $i \in \omega$.*

b) *Es ist $\bigcup_{i\in\omega} U_i = Z(p^\infty)$.*

c) *Es ist $U_i = (\frac{1}{p^i} + R)R$ für alle i.*

d) *Ist V ein Teilmodul von $Z(p^\infty)$, so ist entweder $V = Z(p^\infty)$, oder es gibt ein $i \in \omega$ mit $V = U_i$.*

Beweis. a), b) und c) sind banal zu beweisen. d) Es sei V ein von $Z(p^\infty)$ verschiedener Teilmodul. Es gibt dann eine natürliche Zahl n und ein $r \in R$ mit $\frac{r}{p^n} + R \notin V$. Unter all diesen n gibt es ein kleinstes, welches wir wiederum mit n bezeichnen. Es folgt, dass $U_{n-1} \subseteq V$ ist. Ist andererseits $\frac{x}{p^m} + R \in V$, so dürfen wir annehmen, dass p kein Teiler von x ist. Weil p ein Primelement ist, ist dann x zu p^m teilerfremd, so dass es Elemente u und v in R gibt mit $1 = ux + p^m v$. Hieraus folgt $\frac{1}{p^m} + R \in V$. Dies hat $U_m \subseteq V$ zur Folge. Also ist $m \le n-1$ und daher

$$\frac{x}{p^m} + R \in U_m \subseteq U_{n-1}.$$

Folglich ist $V \subseteq U_{n-1}$. Damit ist auch d) bewiesen.

9.2. Satz. *Es sei R ein Hauptidealbereich und p sei ein Primelement von R. Ist dann α ein Element des Endomorphismenringes R_p des Prüfermoduls $Z(p^\infty)$, so gilt $\alpha(U_i) \subseteq U_i$ für alle $i \in \omega$. Dabei sei U_i wie in 9.1 definiert.*

Beweis. Es sei $x \in U_i$. Dann ist $p^i\alpha(x) = \alpha(p^i x) = 0$. Also ist $\alpha(x) \in U_i$.

9.3. Satz. *Es sei R ein Hauptidealbereich und p sei ein Primelement von R. Wir setzen $a_i := \frac{1}{p^i} + R$ für alle $i \in \omega^*$, wobei $\omega^* := \omega - \{0\}$ gesetzt wurde. Ist dann α ein Element des Endomorphismenringes R_p von $Z(p^\infty)$, so gibt es eine Abbildung f von ω^* in R mit $\alpha(a_i) = f_i a_i$ und $f_{i+1} \equiv f_i \bmod p^i$ für alle $i \in \omega^*$. Ist umgekehrt f eine Abbildung von ω^* in R und gilt $f_{i+1} \equiv f_i \bmod p_i$ für alle $i \in \omega^*$, so gibt es genau ein $\alpha \in R_p$ mit $\alpha(a_i) = f_i a_i$.*

Beweis. Nach 9.2 ist $\alpha(U_i) \subseteq U_i$ für alle $i \in \omega^*$. Daher ist die Menge aller $r \in R$ mit $\alpha(a_i) = ra_i$ nicht leer, so dass es auf Grund des Auswahlaxioms eine Abbildung f von ω^* in R gibt mit $\alpha(a_i) = f_i a_i$ für alle i. Es folgt

$$pf_i a_{i+1} = f_i a_i = \alpha(a_i) = \alpha(pa_{i+1}) = pf_{i+1}a_{i+1}$$

und damit

$$pf_i \equiv pf_{i+1} \bmod p^{i+1},$$

dh.,

$$f_i \equiv f_{i+1} \bmod p^i.$$

Es sei umgekehrt f eine Abbildung von ω^* in R und es gelte $f_i \equiv f_{i+1} \bmod p^i$ für alle $i \in \omega^*$. Mittels Induktion folgt die Gültigkeit von

$$f_i \equiv f_{i+k} \bmod p^i$$

für alle i, $k \in \omega^*$. Wir definieren eine binäre Relation α auf $Z(p^\infty)$ durch $(u,v) \in \alpha$ genau dann, wenn es ein $x \in R$ und ein $i \in \omega^*$ gibt mit $u = xa_i$ und $v = xf_ia_i$. Sind (u,v), $(u,w) \in \alpha$, so ist also $u = xa_i$, $v = xf_ia_i$, $u = ya_k$ und $w = yf_ka_k$ für passende x, y, i und k. Es sei oBdA $i \leq k$. Dann ist $xp^{k-i}a_k = u = ya_k$ und daher

$$y \equiv xp^{k-i} \bmod p^k.$$

Andererseits ist $f_k \equiv f_i \bmod p^i$ und daher

$$f_kp^{k-i} \equiv f_ip^{k-i} \bmod p^k.$$

Folglich ist

$$yf_k \equiv xp^{k-i}f_k \equiv xp^{k-i}f_i \bmod p^k.$$

Hiermit folgt

$$v \equiv xf_ia_i = xf_ip^{k-i}a_k = yf_ka_k = w.$$

Ist andererseits $u \in Z(p^\infty)$, so gibt es nach 9.1 ein $x \in R$ und ein $i \in \omega^*$ mit $u = xa_i$. Daher ist $(u, xf_ia_i) \in \alpha$. Damit ist α als Abbildung von $Z(p^\infty)$ in sich erkannt.

Es seien u, $v \in Z(p^\infty)$. Es gibt dann x, $y \in R$ und i, $k \in \omega^*$ mit $u = xa_i$ und $v = ya_k$. Es sei oBdA $i \leq k$. Dann ist

$$\begin{aligned}\alpha(u+v) &= \alpha\big((xp^{k-i}+y)a_k\big)\\ &= (xp^{k-i}+y)f_ka_k\\ &= xf_ka_i + yf_ka_k.\end{aligned}$$

Wegen $f_i \equiv f_k \bmod p^i$ folgt weiter $\alpha(u+v) = \alpha(u) + \alpha(v)$, so dass α additiv ist. Ist $r \in R$, so folgt auch noch

$$\alpha(ru) = rxf_ia_i = r\alpha(u),$$

so dass α in der Tat ein Endomorphismus mit den verlangten Eigenschaften ist. Die Einzigkeit von α folgt aus der Bemerkung, dass die Menge der a_i ein Erzeugendensystem von $Z(p^\infty)$ ist.

9.4. Satz. *Es sei R ein Hauptidealbereich und p sei ein Primelement von R. Sind α, $\beta \in R_p$ und werden α und β gemäß 9.3 durch die beiden Abbildungen*

f und g von ω^* in R dargestellt, so werden $\alpha + \beta$ und $\alpha\beta$ durch $f + g$ bzw. fg dargestellt, wobei Summe und Produkt von f mit g punktweise definiert sei. Insbesondere folgt, dass R_p kommutativ ist.

Beweis. Banal.

9.5. Satz. *Es sei R ein Hauptidealbereich und p sei ein Primelement von R. Wir definieren $\pi \in R_p$ durch $\pi(x) := px$ für alle $x \in Z(p^\infty)$. Ist dann Q ein von $\{0\}$ verschiedenes Ideal von R_p und ist $V := \bigcap_{\alpha \in Q} \mathrm{Kern}(\alpha)$, so ist $V = U_n$ mit einem $n \in \omega$ und $Q = \pi^n R_p$.*

Beweis. Weil V ein Teilmodul von $Z(p^\infty)$ ist, ist nach 9.1 entweder $V = Z(p^\infty)$ oder $V = U_n$ mit einem passenden n. Weil $Q \neq \{0\}$ ist, kann der erste Fall nicht eintreten. Also ist $V = U_n$.

Es sei $0 \neq \alpha Q$ und U_m sei der Kern von α. Dann ist $n \leq m$. Es werde α gemäß 9.3 durch die Abbildung f dargestellt. Dann ist $f_m \equiv 0 \bmod p^m$ und daher $f_{m+i} \equiv 0 \bmod p^m$ für alle $i \in \omega^*$. Andererseits ist f_{m+i} für alle $i \in \omega^*$ nicht durch p^{m+1} teilbar, da sonst a_{m+1} wegen $f_{m+i} \equiv f_{m+1} \bmod p^{m+1}$ im Kern von α läge. Insbesondere ist also $f_{m+i} \neq 0$ für alle $i \in \omega^*$. Es gibt daher zu jedem $i \in \omega^*$ genau ein $r_i \in R$ mit $f_{m+i} = r_i p^m$. Es folgt $r_{i+1}p^m \equiv r_i p^m \bmod p^{m+1}$, was die Kongruenz $r_{i+1} \equiv r_i \bmod p^i$ nach sich zieht. Nach 9.3 wird also durch $\rho(a_i) := r_i a_i$ ein $\rho \in R_p$ definiert. Nun ist

$$\rho\pi^m(a_i) = \rho(p^m a_i) = 0 = \alpha(a_i),$$

falls $i \leq m$ ist. Andererseits ist

$$\rho\pi_m(a^{m+i}) = \rho(a_i) = r_i a_i = r_i p^m a_{m+i} = \alpha(a_{m+i})$$

für alle $i > 0$. Also ist $\rho\pi^m = \alpha$. Wäre nun ρ keine Einheit, so wäre $U_1 \subseteq \mathrm{Kern}(\rho)$, was wegen $r_1 \not\equiv 0 \bmod p$ nicht der Fall ist. Weil Q ein Ideal ist, ist also $\pi^m \in Q$.

Es sei nun k das kleinste unter allen $m \in \omega$ mit $\pi^m \in Q$. Dann gibt es also zu jedem $\alpha \in Q$ ein $\sigma \in R_p$ mit $\alpha = \sigma\pi^k$. Also ist

$$Q \subseteq \pi^k R_p \subseteq Q.$$

Folglich ist $Q = \pi^k R_p$. Dann ist aber $U_n = \mathrm{Kern}(\pi^k)$ und damit $k = n$, was zu beweisen war.

Der Beweis von 9.5 liefert auch noch den folgenden Satz.

9.6. Satz. *Es sei R ein Hauptidealbereich und p sei ein Primelement von R. Es sei weiter π der durch $\pi(x) := px$ definierte Endomorphismus von $Z(p^\infty)$. Ist dann $0 \neq \alpha \in R_p$, so gibt es eine Einheit ρ in R_p und ein $n \in \omega$ mit $\alpha = \rho\pi^n$.*

Weil Einheiten stets bijektiv sind und π offensichtlich surjektiv ist, gilt auch

9.7. Korollar. *Jeder von Null verschiedene Endomorphismus von $Z(p^\infty)$ ist surjektiv.*

Weil das Produkt zweier surjektiver Abbildungen surjektiv ist, haben wir ferner

9.8. Korollar. *Die Ringe R_p sind Integritätsbereiche.*

Da R_p Integritätsbereich ist, existiert der Quotientenkörper $Q(R_p)$. Um ein hinreichendes Kriterium dafür zu erhalten, dass gewisse dieser Körper nicht isomorph sind, untersuchen wir nun die Gruppen von Einheitswurzeln in R_p. Bevor wir dies tun, sei noch darauf hingewiesen, dass R_p der Ring der ganzen henselschen p-adischen Zahlen ist, falls R der Ring der ganzen Zahlen ist. In diesem Falle ist $Q(R_p)$ der Körper der henselschen p-adischen Zahlen.

9.9. Satz. *Es sei R ein Hauptidealbereich und p sei ein Primelement von R. Ist $\sigma \in R_p$ und wird σ gemäß 9.3 durch f dargestellt, so setzen wir $\psi(\sigma) := f_i + p^i R$. Dann ist ψ ein Epimorphismus von R_p auf R/p^iR. Ferner gilt* $\mathrm{Kern}(\psi) = \pi^i R_p$, *so dass $R_p/\pi^i R_p$ und R/p^iR isomorph sind.*

Beweis. Wird σ gemäß 9.3 auch durch g dargestellt, so ist $g_i \equiv f_i \bmod p^i$, so dass ψ wohldefiniert ist. Dann ist aber klar, dass ψ ein Homomorphismus ist.

Ist $r \in R$, so wird durch $\rho(x) := rx$ für alle $x \in Z(p^\infty)$ ein $\rho \in R_p$ definiert. Wegen $\psi(\rho) = r + p^iR$ ist ψ auch surjektiv.

Es sei $\psi(\sigma) = 0$. Dann ist $f_i \equiv 0 \bmod p^i$. Ist $\sigma \neq 0$, so gibt es nach 9.6 eine Einheit τ in R_p und ein $m \in \omega$ mit $\sigma = \tau\pi^m$. Wird τ durch t dargestellt, so folgt $f_i \equiv t_i p^m \bmod p^i$. Weil τ eine Einheit ist, ist t_i nicht durch p teilbar. Wegen $f_i \equiv 0 \bmod p^i$ ist daher $i \leq m$, womit alles bewiesen ist.

9.10. Satz. *Es sei R ein Hauptidealbereich und p sei ein Primelement von R. Mit $W(R_p)$ bezeichnen wir die Gruppe der Einheitswurzeln von R_p, dh., die Torsionsgruppe der Einheitengruppe von R_p. Setzt man*

$$\varphi(\epsilon) := \epsilon + \pi R_p$$

für alle $\epsilon \in W(R_p)$, so ist π ein Epimorphismus von $W(R_p)$ auf die Gruppe der Einheitswurzeln $W(R_p/\pi R_p)$ des Körpers $R_p/\pi R_p$.

Beweis. Es sei $\epsilon \in W(R_p)$ und es gelte $\epsilon^n = 1$. Dann ist $\varphi(\epsilon)^n = \varphi(\epsilon^n) = 1$, so dass φ ein Homomorphismus in $W(R_p/\pi R_p)$ ist.

Um die Surjektivität von φ zu beweisen, sei n die Ordnung des Elementes $\eta + \pi R_p \in W(R_p/\pi R_p)$. Wendet man 9.9 mit $i = 1$ an, so folgt die Existenz eines $f_1 \in R$ mit $\psi(\eta) = f_1 + pR$. Es folgt, dass die Ordnung von $f_1 + pR$ gleich n ist. Insbesondere ist also $f_1^n \equiv 1 \bmod p$. Es sei $i \geq 1$ und es gebe $f_1, \ldots, f_i \in R$ mit $f_{j+1} \equiv f_j \bmod p^j$ und $f_j^n \equiv 1 \bmod p^j$ für alle $j \leq i$. Insbesondere ist dann $f_i^n = 1 + kp^i$ mit einem $k \in R$. Ist die Charakteristik q von R/pR ungleich 0, so hat R/pR nur die triviale q-te Einheitswurzel 1, so dass q kein Teiler von n ist. Dann ist aber p kein Teiler von $q \cdot 1$, wobei 1 die Eins von R bezeichne. Weil auch f_i zu p teilerfremd ist, gibt es ein $v \in R$ mit

$$nf_i^{n-1}v \equiv -k \bmod p.$$

Es folgt weiter

$$nf_i^{n-1}vp^i + kp^i \equiv 0 \bmod p^{i+1}.$$

Setze $f_{i+1} := f_i + vp^i$. Dann ist $f_{i+1} \equiv f_i \bmod p^i$ und

$$\begin{aligned} f_{i+1}^n &\equiv f_i^n + nvp^i f_i^{n-1} \\ &\equiv 1 + kp^i + nvp^i f_i^{n-1} \\ &\equiv 1 \bmod p^{i+1}. \end{aligned}$$

Damit ist — auf die übliche, aber schlampige Weise — die Existenz einer Abbildung f der natürlichen Zahlen in R sichergestellt mit $f_{i+1} \equiv f_i \bmod p^i$ und $f_i^n \equiv 1 \bmod p^i$ für alle i. Nach 9.3 gibt es nun ein $\epsilon \in R_p$, welches durch f dargestellt wird. Es folgt

$$\epsilon^n = 1$$

sowie

$$\psi(\epsilon) = f_1 + pR = \psi(\eta)$$

und damit

$$\varphi(\epsilon) = \epsilon + \pi R_p = \eta + \pi R_p,$$

womit auch die Surjektivität von φ nachgewiesen ist.

Ist R ein Integritätsbereich, so erbt R von seinem Quotientenkörper $Q(R)$ die Charakteristik, da R ja zu einem Teilring von $Q(R)$ isomorph ist.

9.11. Satz. *Es sei R ein Hauptidealbereich und p sei ein Primelement von R. Ferner sei φ der in 9.10 definierte Epimorphismus von $W(R_p)$ auf $W(R_p/\pi R_p)$. Ist* $\mathrm{Kern}(\varphi) \neq \{1\}$*, so ist die Charakteristik von R gleich* 0 *und die Charakteristik q von $R_p/\pi R_p$ ist größer als* 0*. Überdies ist p ein Teiler von $q \cdot 1$, wobei* 1 *die Eins von R bezeichne.*

Beweis. Es sei $1 \neq \alpha \in \mathrm{Kern}(\varphi)$ und n sei die Ordnung von α. Ferner sei q eine n teilende Primzahl. Setze $\beta := \alpha^{n/q}$. Dann ist β ein Element der Ordnung q im Kern von φ. Es gibt daher ein $\rho \in R_p$ mit $\beta = 1 + \rho\pi$. Es folgt

$$1 = \beta^q = 1 + \sum_{i=1}^{q} \binom{q}{i} \rho^i \pi^i.$$

Weil R_p nullteilerfrei ist, folgt hieraus

$$q \cdot 1 \equiv 0 \bmod \pi.$$

Daher ist q die Charakteristik von $R_p/\pi R_p$ und es folgt, dass $\mathrm{Kern}(\varphi)$ eine q-Gruppe ist. Wäre die Charakteristik von R_p nicht Null, so wäre sie gleich q. Es folgte

$$1 = \beta^q = (1 + \rho\pi)^q = 1 + \rho^q \pi^q$$

und damit $\rho^q \pi^q = 0$, so dass $\rho = 0$ wäre im Widerspruch zu $\beta \neq 1$. Damit ist der Satz in allen seinen Teilen bewiesen.

Ist R ein Hauptidealbereich, so erbt R, wie schon bemerkt, von $Q(R)$ die Charakteristik. Ist diese positiv, so hat auch R/pR diese Charakteristik, falls nur p ein Primelement von R ist. Ist R/pR endlich, so können wir R_p auf eine andere Art darstellen, die das Isomorphieproblem in diesem Falle löst. Genaueres sagt der nächste Satz.

9.12. Satz. *Es sei R ein Hauptidealbereich der Charakteristik $q > 0$. Ist p ein Primelement von R und ist R/pR algebraisch über seinem Primkörper, so ist der Endomorphismenring R_p von $Z(p^\infty)$ dem Ring der formalen Potenzreihen über R/pR isomorph.*

Beweis. Weil R/pR zu $R_p/\pi R_p$ isomorph ist, ist auch dieser Körper algebraisch über seinem Primkörper, der zu $\mathrm{GF}(q)$ isomorph ist. Dies impliziert, dass der Körper $R_p/\pi R_p$ die Vereinigung der in ihm enthaltenen endlichen Teilkörper ist. Hieraus folgt wiederum

$$W(R_p/\pi R_p) = (R_p/\pi R_p)^*.$$

Setze $K := W(R_p) \cup \{0\}$. Wir zeigen, dass K ein Körper ist. Da K offensichtlich multiplikativ abgeschlossen ist, müssen wir nur noch zeigen, dass K auch additiv abgeschlossen ist. Dazu seien α und β zwei von 0 verschiedene Elemente aus K. Dann sind $\alpha + \pi R_p$ und $\beta + \pi R_p$ von Null verschiedene Elemente von $R_p/\pi R_p$, die überdies in einem endlichen Teilkörper von $R_p/\pi R_p$ liegen. Dieser habe die Ordnung q^n. Dann gilt

$$(\alpha + \pi R_p)^{q^n-1} = 1 + \pi R_p$$

und

$$(\beta + \pi R_p)^{q^n-1} = 1 + \pi R_p.$$

Wegen 9.10 und 9.11 ist dann $\alpha^{q^n-1} = 1$ und $\beta^{q^n-1} = 1$. Hieraus folgt weiter $\alpha^{q^n} = \alpha$ und $\beta^{q^n} = \beta$. Weil q auch die Charakteristik von R_p ist, folgt schließlich

$$(\alpha + \beta)^{q^n} = \alpha + \beta.$$

Ist nun $\alpha + \beta = 0$, so ist nichts zu beweisen. Ist dies nicht der Fall, so folgt

$$(\alpha + \beta)^{q^n-1} = 1$$

und damit $\alpha + \beta \in K$. Folglich ist K ein Körper. Weil $K \cap \pi R_p = \{0\}$ ist, folgt schließlich, dass K zu $R_p/\pi R_p$ isomorph ist.

Offensichtlich gilt $\bigcap_{n:=1}^{\infty} \pi^n R_p = \{0\}$. Nimmt man diese Ideale als Umgebungsbasis der Null, so erhält man eine hausdorffsche Topologie T auf R_p, die R_p zu einem topologischen Ring macht. Das Element π ist transzendent über K. Ist nämlich n eine natürliche Zahl, sind n und $k_0, \ldots, k_n \in K$ und gilt $0 = \sum_{i:=0}^{n} k_i \pi^i$, so folgt wegen $K \cap \pi R_p = \{0\}$ zunächst $k_0 = 0$ und dann mittels Induktion $k_i = 0$ für $i := 1, \ldots, n$. Somit ist $K[\pi]$ zum Polynomring in einer Unbestimmten über K isomorph. Mit $K_n[\pi]$ bezeichnen wir die Menge der Polynome in π, deren Grad n nicht übersteigt. Dann ist

$$R_p = K_n[\pi] \oplus \pi^{n+1} R_p.$$

Dies folgt mit einer leichten Induktion über n. Zu jedem $r \in R_p$ und zu jedem $n \in \omega$ gibt es also genau ein $c_n \in K_n[\pi]$ mit

$$r \equiv c_n \bmod \pi^{n+1}.$$

Es folgt, dass c bez. der Topologie T eine Cauchyfolge ist und dass $r = \lim c$ gilt. Dies impliziert, dass R_p ein Teilring des Rings $K[[\pi]]$ der formalen Potenzreihen über K ist. Wir müssen nun nur noch zeigen, dass jede Cauchyfolge über $K[\pi]$ in R_p konvergiert.

Um dies zu zeigen, sei c eine Cauchyfolge über $K[\pi]$. Es sei $n \in \omega$. Es gibt dann ein $M \in \omega$ mit

$$c_u - c_v \in \pi^n R_p$$

für alle u und v mit $u, v \geq M$. Setzt man wieder $a_i := \frac{1}{\pi^i} + R$, so ist also

$$c_u(a_i) = c_v(a_i)$$

für alle $i \leq n$ und alle $u, v \geq M$. Es sei $M(n)$ das kleinste unter diesen M. Dann ist $M(n) \leq M(n+1)$ für alle n. Es gibt ferner $r_1, \ldots, r_n \in R$ mit

$$c_u(a_i) = r_i a_i$$

für alle $i \geq n$ und alle $u \leq M(n)$. Es gibt also eine Auswahlfunktion F, die jedem n ein n-Tupel F_n von Elementen aus R zuordnet, so dass

$$c_u(a_i) = F_{n,i} a_i$$

gilt für alle $i \leq n$ und alle $u \geq M(n)$. Definiere f durch $f_n := F_{n,n}$. Dann ist $c_u(a_n) = f_n a_n$ für alle $u \geq M(n)$. Wegen $M(n+1) \geq M(n)$ ist dann

$$\begin{aligned} f_{n+1} a_n &= f_{n+1} p a_{n+1} \\ &= p c_{M(n+1)}(a_{n+1}) \\ &= c_{M(n+1)}(a_n) \\ &= c_{M(n)}(a_n) \\ &= f_n a_n. \end{aligned}$$

Hieraus folgt

$$f_{n+1} \equiv f_n \bmod p^n,$$

so dass es nach 9.3 ein Element $\rho \in R_p$ gibt mit $\rho(a_n) = f_n a_n$ für alle n. Es folgt

$$(\rho - c_u) a_n = f_n a_n - F_{n,n} a_n = 0$$

für alle $u \geq M(n)$ und damit

$$\rho - c_u \in \pi^n R_p$$

für alle $u \geq M(n)$, so dass $\lim c = \rho$ gilt. Damit ist alles bewiesen.

9.13. Korollar *Es sei R Hauptidealbereich mit von Null verschiedener Charakteristik. Ist p ein Primelement von R und ist R/pR algebraisch über seinem Primkörper, so ist der Quotientenkörper $Q(R_p)$ von R_p isomorph zum Körper der formalen Laurentreihen über R/pR.*

Beweis. Dies folgt unmittelbar aus 9.12 und der Bemerkung, dass der Quotientenkörper des Ringes der formalen Potenzreihen über einem Körper der Körper der formalen Laurentreihen über eben diesem Körper ist.

9.14. Satz. *Es seien R und S Hauptidealbereiche mit von Null verschiedener Charakteristik. Ferner seien p und q Primelemente von R bzw. S. Ist R/pR algebraisch über seinem Primkörper, so sind die folgenden Aussagen äquivalent:*

a) *Die Ringe R_p und S_q sind isomorph.*

b) *Die Körper $R_p/\pi R_p$ und $S_q/\rho S_q$ sind isomorph. Dabei seien mit πR_p und ρS_q die maximalen Ideale der Ringe R_p bzw. S_q bezeichnet.*

c) *Die Ringe R/pR und S/qS sind isomorph.*

d) *Der Körper $S_q/\rho S_q$ ist algebraisch über seinem Primkörper und die Quotientenkörper $Q(R_p)$ und $Q(S_q)$ von R_p bzw. S_q sind isomorph.*

Beweis. a) impliziert b). Jeder Isomorphismus von R_p auf S_q bildet das maximale Ideal πR_p von R_p auf das maximale Ideal ρS_q von S_q ab und induziert daher einen Isomorphismus von $R_p/\pi R_p$ auf $S_q/\rho S_q$.

b) impliziert c). Weil R/pR zu $R_p/\pi E_p$ und S/qS zu $S_q/\rho S_q$ isomorph ist, sind R/pR und S/qS isomorph.

c) impliziert a). Sind R/pR und S/qS isomorph, so sind es auch $R_p/\pi R_p$ und $S_q/\rho S_q$. Weil R/R_p über seinem Primkörper algebraisch ist, gilt dies daher auch für die zuletzt genannten Körper. Weil die Charakteristiken von R und S von Null verschieden sind, sind nach 9.12 die Ringe R_p und S_q folglich zu den Ringen von formalen Potenzreihen über $R_p/\pi R_p$ bzw. über $S/\rho S_q$ isomorph. Daher sind R_p und S_q isomorph.

Isomorphe Integritätsbereiche haben natürlich isomorphe Quotientenkörper. Wir müssen daher nur noch zeigen, dass a) eine Folge von d) ist. Hierzu müssen wir auf den Satz zurückgreifen, dass Hauptidealbereiche — und R_p und S_q sind ja solche — in ihren Quotientenkörpern ganz abgeschlossen sind. Dies bedeutet, dass die in $Q(R_p)$ liegenden Nullstellen eines Polynoms aus $R_p[x]$, dessen Leitkoeffizient 1 ist, in R_p liegen. Dies zu beweisen, sei dem Leser als Übungsaufgabe überlassen. Es ist eine einfache Folgerung aus dem Satz über die eindeutige Primfaktorzerlegung, der ja in Hauptidealbereichen gilt. Aus der Tatsache, dass R_p und S_q in ihren Quotientenkörpern ganz abgeschlossen sind, folgt, dass $W(Q(R_p)) = W(R_p)$ und $W(Q(S_q)) = W(S_q)$ ist.

Es sei nun α ein Isomorphismus von $Q(R_p)$ auf $Q(S_q)$, also $\alpha(W(R_p)) = W(S_q)$. Setzt man $K := W(R_p) \cup \{0\}$ und $L := W(S_q) \cup \{0\}$, so induziert α einen Isomorphismus des Körpers K auf den Körper L. Weil sowohl $R_p/\pi R_p$ als auch $S_q/\rho S_q$ über ihren Primkörpern algebraisch sind, sind die Körper $R_p/\pi R_p$ und $S_q/\rho S_q$ isomorph, so dass b) und damit a) eine Folge von d) ist. Damit ist alles bewiesen.

Mit den Sätzen 9.13 und 9.14 erhalten wir daher zu jeder von 0 verschiedenen Charakteristik überabzählbar viele Beispiele von Körpern $Q(R_p)$, da GF(r) für jede Primzahl r überabzählbar viele, nicht isomorphe, algebraische Erweiterungen besitzt (Steinitz 1910).

Mit Z bezeichnen wir im folgenden den Ring der ganzen Zahlen.

9.15. Satz. *Es sei p eine Primzahl im Ring Z der ganzen Zahlen. Dann ist $|W(Z_p)| = p - 1$, es sei denn, es ist $p = 2$. In diesem Falle gilt $|W(Z_2)| = 2$.*

Beweis. Es sei φ der in 9.10 definierte Epimorphismus von $W(Z_p)$ auf GF$(p)^*$. Ferner sei $1 \neq \alpha \in \mathrm{Kern}(\varphi)$. Nach 9.11 ist dann $o(\alpha) = p^n$ mit einer natürlichen Zahl n. Wir setzen $\beta := \alpha^{p^{n-1}}$. Dann ist $o(\beta) = p$. Es werde β entsprechend 9.3 durch f dargestellt, wobei wir annehmen dürfen, dass $0 \leq f_i < p^i$ ist für alle i. Es folgt

$$f_i^p \equiv 1 \bmod p^i$$

für alle i. Insbesondere folgt $f_1 = 1$. Es sei m die kleinste natürliche Zahl, für die $f_{m+1} \neq 1$ gilt. Dann ist

$$f_{m+1} = f_m + vp^m = 1 + vp^m.$$

Wegen $1 < f_{m+1} < p^{m+1}$ folgt $0 < v < p$. Nun ist

$$f_{m+2} = f_{m+1} + wp^{m+1}$$

und daher

$$1 \equiv f_{m+2}^p \equiv f_{m+1}^p + pf^{p-1}wp^{m+1} \equiv f_{m+1}^p \bmod p^{m+2}.$$

Wäre $m \geq 2$, so folgte weiter

$$1 \equiv (1 + vp^m)^p \equiv 1 + pvp^m \bmod p^{m+2}$$

und dann

$$0 \equiv vpm + 1 \bmod p^{m+2},$$

so dass

$$0 \equiv v \bmod p$$

wäre im Widerspruch zu $0 < v < p$. Also ist $m = 1$. Dann ist aber

$$1 \equiv 1 + pvp + \binom{p}{2} v^2 p^2 \bmod p^3$$

und weiter

$$0 \equiv pvp + \binom{p}{2} v^2 p^2 \bmod p^3.$$

Wäre $p > 2$, so wäre $\binom{p}{2}$ durch p teilbar, und es folgte wieder der Widerspruch $v \equiv 0 \bmod p$. Also ist $p = 2$.

Es bleibt uns noch zu zeigen, dass $\alpha = -1$ ist. Um dies zu zeigen, müssen wir zeigen, dass $n = 1$ ist. Dazu werde α gemäß 9.3 durch g dargestellt. Weil $\beta^2 = 1 \neq \beta$ ist, ist $\beta = -1$, dh., es ist $\alpha^{2^{n-1}} = -1$. Daher gilt insbesondere

$$g_2^{2^{n-1}} \equiv -1 \bmod 4.$$

Da -1 kein Quadrat modulo 4 ist, folgt hieraus $n = 1$, so dass in der Tat $\alpha = -1$ ist. Damit ist alles bewiesen.

9.16. Satz. *Es seien p und q zwei Primzahlen des Ringes Z der ganzen Zahlen. Genau dann sind die Quotientenkörper $Q(Z_p)$ und $Q(Z_q)$ isomorph, wenn $p = q$ ist.*

Beweis. Ist $p = q$, so ist nichts zu beweisen. Wir nehmen daher an, dass die fraglichen Körper isomorph seien. Es gilt wieder $W(Z_p) = W(Q(Z_p))$ und $W(Z_q) = W(Q(Z_q))$. Aus der Isomorphie von $Q(Z_p)$ und $Q(Z_q)$ folgt natürlich die Isomorphie $W(Z_p)$ und $W(Z_q)$, so dass mit 9.15 entweder $p-1 = q-1$ und damit $p = q$ oder aber, falls wir $q < p$ annehmen, $q = 2$ und $p = 3$ folgt.

Um zu zeigen, dass $Q(Z_2)$ und $Q(Z_3)$ nicht isomorph sind, zeigen wir, dass das Polynom $x^3 + x + 1$ in $Q(Z_3)$ eine Nullstelle hat, in $Q(Z_2)$ aber nicht. Letzteres ist sofort zu sehen. Wäre nämlich ζ eine Nullstelle dieses Polynoms in $Q(Z_2)$, so läge ζ in Z_2, da Z_2 ja ganz abgeschlossen ist. Dann wäre aber $\zeta + \pi Z_2$ eine Nullstelle dieses Polynoms über GF(2) im Widerspruch zu der Tatsache, dass dieses Polynom über GF(2) nur den Wert 1 annimmt.

Setze $f_1 := 1$. Dann ist $f_1^3 + f_1 + 1 \equiv 0 \bmod 3$. Es sei $n \geq 1$ und es gebe $f_i \in Z_3$ mit $f_i^3 + f_i + 1 \equiv 0 \bmod 3$ für alle $i \leq n$, für die außerdem noch gilt, dass $f_{i+1} \equiv f_i \bmod 3^i$ ist für alle $i < n$. Es gibt dann ein $k \in Z$ mit $f_n^3 + f_n + 1 = k3^n$. Setze $f_{n+1} := f_n - k3^n$. Dann gilt zum einen $f_{n+1} \equiv f_n \bmod 3^n$ und zum Anderen

$$f_{n+1}^3 = f_n^3 - 3f_n^2 k 3^n + 3f_n k^2 3^{2n} - k^3 3^{3n} \equiv f_n^3 \bmod 3^{n+1}.$$

Daher ist

$$f_{n+1}^3 + f_{n+1} + 1 \equiv f_n^3 + f_n - k3^n + 1 = 0 \bmod 3^{n+1}.$$

Nach 9.3 folgt die Existenz eines $\eta \in Z_3$ mit $\eta(a_n) = f_n a_n$. Dann ist aber

$$(\eta^3 + \eta + 1)(a_n) = (f_n^3 + f_n + 1)a_n = 0,$$

so dass η in der Tat eine Nullstelle von $x^3 + x + 1$ ist. Damit ist auch gezeigt, dass auch $Q(Z_2)$ und $Q(Z_3)$ nicht isomorph sind.

Dem Kenner wird nicht verborgen geblieben sein, dass wir in den Beweisen des letzten Satzes und des Satzes 9.10 Spezialfälle des henselschen Lemmas etabliert haben. Dem, der dieses Lemma nicht kennt, sei als gute Übungsaufgabe empfohlen, dieses Lemma aus den beiden Beweisen herauszupräparieren und zu beweisen. Als Hinweis sei erwähnt, dass das henselsche Lemma eine Aussage über die Faktorisierung von Polynomen macht. Die hier über die Existenz von

Nullstellen gewisser Polynome gemachten Aussagen muss man also als Teilbarkeit durch Polynome (ersten Grades) interpretieren.

Wir sind nun in der Lage, nicht isomorphe Quaternionenschiefkörper *en masse* zu konstruieren.

9.17. Satz. *Es sei R ein Hauptidealbereich und p sei ein Primelement von R. Ferner sei $c \in R_p$ und das Polynom $x^2 + x - c$ sei aufgefasst als Polynom über $R_p/\pi R_p$ irreduzibel. Ist dann H_p der Zentralisator der beiden Matrizen*

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ c & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & c & 1 \end{pmatrix} \quad \textit{und} \quad \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & -1 \\ \pi & 0 & 0 & 0 \\ \pi & -\pi & 0 & 0 \end{pmatrix}$$

im Ring der (4×4)-Matrizen über $Q(R_p)$, so ist H_p ein Quaternionenschiefkörper mit $Z(H_p) \cong Q(R_p)$. Überdies besteht H_p gerade aus den Matrizen

$$\begin{pmatrix} \alpha & \beta & \gamma & \delta \\ c\beta & \alpha + \beta & c\delta & \gamma + \delta \\ \pi(\gamma + \delta) & -\pi\delta & \alpha + \beta & -\beta \\ -\pi c\delta & \pi\gamma & -c\beta & \alpha \end{pmatrix}$$

mit α, β, γ, $\delta \in Q(R_p)$.

Beweis. Für den Erfahrenen ist es eine langweilige, für den Ungeübten eine nützliche und darüber hinaus eine gehaltvolle Übung in Matrizenmultiplikation nachzuweisen, dass H_p gerade aus den zuletzt genannten Matrizen besteht. Man sieht dann, dass man diese Matrizen mit ihrer ersten Zeile identifizieren kann. Sind $(\alpha, \beta, \gamma, \delta)$ und $(\alpha', \beta', \gamma', \delta')$ zwei dieser Zeilen, so ergibt sich die erste Zeile des Produktes ihrer zugehörigen Matrizen zu

$$\begin{aligned} \alpha'' &= \alpha\alpha' + c\beta\beta' + \pi\gamma\gamma' + \pi\gamma\delta' - \pi c\delta\delta', \\ \beta'' &= \alpha\beta' + \alpha'\beta + \beta\beta' - \pi\gamma\delta' + \pi\gamma'\delta, \\ \gamma'' &= \alpha\gamma' + c\beta\delta' + \gamma\alpha' + \gamma\beta' - c\delta\beta', \\ \delta'' &= \alpha\delta' + \beta\gamma' + \beta\delta' - \gamma\beta' + \delta\alpha'. \end{aligned}$$

Die Elemente $(\zeta, 0, 0, 0)$ liegen natürlich im Zentrum von H_p, da sie ja Diagonalmatrizen darstellen, deren Hauptdiagonaleinträge alle gleich ζ sind. Es sei $(\zeta_1, \zeta_2, \zeta_3, \zeta_4)$ ein Element des Zentrums. Dann ist

$$(\zeta_1, \zeta_2, \zeta_3, \zeta_4)(0, 1, 0, 0) = (c\zeta_2, \zeta_1 + \zeta_2, \zeta_3 - c\zeta_4, -\zeta_3)$$

und

$$(0, 1, 0, 0)(\zeta_1, \zeta_2, \zeta_3, \zeta_4) = (c\zeta_2, \zeta_1 + \zeta_2, c\zeta_4, \zeta_3 + \zeta_4).$$

Koeffizientenvergleich liefert $\zeta_3 = 2c\zeta_4$ und $\zeta_4 = -2\zeta_3$. Hieraus folgt $\zeta_3 = -4c\zeta_3$. Wäre ζ_3 nicht Null, so folgte $-c = \frac{1}{4}$ und damit

$$x^2 + x - c = \left(x + \frac{1}{2}\right)^2,$$

so dass dieses Polynom über $R_p/\pi R_p$ nicht irreduzibel wäre. Also ist $\zeta_3 = 0$ und damit auch $\zeta_4 = 0$.

Weiter folgt

$$(\zeta_1, \zeta_2, 0, 0)(0, 0, 1, 0) = (0, 0, \zeta_1, \zeta_2)$$

und

$$(0, 0, 1, 0)(\zeta_1, \zeta_2, 0, 0) = (0, 0, \zeta_1 + \zeta_2, -\zeta_2),$$

so dass auch $\zeta_2 = 0$ ist. Also besteht $Z(H_p)$ aus genau den Elementen $(\zeta, 0, 0, 0)$.

Es ist

$$(\alpha, \beta, \gamma, \delta)(\alpha + \beta, -\beta, -\gamma, -\delta) = \bigl(\alpha^2 + \alpha\beta - c\beta^2 - \pi(\gamma^2 + \gamma\delta - c\delta^2), 0, 0, 0\bigr).$$

Hieraus folgt, dass die zu $(\alpha, \beta, \gamma, \delta)$ gehörende Matrix sicher dann invertierbar ist, wenn

$$(\alpha^2 + \alpha\beta - c\beta^2 - \pi(\gamma^2 + \gamma\delta - c\delta^2) \neq 0$$

ist. Es sei also

$$(\alpha^2 + \alpha\beta - c\beta^2 - \pi(\gamma^2 + \gamma\delta - c\delta^2) = 0.$$

Indem wir diese Gleichung mit dem Quadrat des Hauptnenners der in sie eingehenden Koeffizienten multiplizieren, sehen wir, dass wir annehmen dürfen, dass sie in R_p liegen. Weil R_p ein Hauptidealring ist, dürfen wir weiter annehmen, dass sie teilerfremd sind, falls sie nicht alle Null sind. Nun ist

$$\alpha^2 + \alpha\beta - c\beta^2 \equiv 0 \bmod \pi.$$

Wegen der vorausgesetzten Irreduzibilität von $x^2 + x - c$ folgt hieraus, dass sowohl α also auch β durch π teilbar ist. Dann ist aber

$$\alpha^2 + \alpha\beta - c\beta^2 \equiv 0 \bmod \pi^2,$$

so dass

$$\gamma^2 + \gamma\delta - c\delta^2 \equiv 0 \bmod \pi,$$

ist. Hieraus folgt, dass auch γ und δ durch π teilbar sind, so dass die Teilerfremdheit von α, β, γ und δ nicht zu erreichen ist. Also sind alle diese Koeffizienten Null, so dass H_p in der Tat ein Körper ist. Da offensichtlich $[H_p : Z(H_p)] = 4$ ist, ist H_p ein Quaternionenschiefkörper. Damit ist alles bewiesen.

In dem gerade bewiesenen Satz steht eine Voraussetzung, deren Realisierbarkeit noch nicht geklärt ist, nämlich die Voraussetzung, dass c ein Element sei, für das $x^2 + x - c$ über $R_p/\pi R_p$ irreduzibel ist. Um die anstehende Frage zu beantworten, betrachten wir einen Körper K der Charakteristik $p > 0$, von dem wir annehmen, dass er algebraisch über seinem Primkörper sei. Wir setzen

$$E(K) := \bigl\{n \mid n \in N, \mathrm{GF}(p^n) \subseteq K\bigr\}.$$

Dabei ist $\mathrm{GF}(p^n) \subseteq K$ so zu verstehen, dass K einen zu $\mathrm{GF}(p^n)$ isomorphen Teilkörper enthalte. Dann hat $E(K)$ die folgenden Eigenschaften:

a) Es ist $1 \in E(K)$.

b) Ist $n \in E(K)$ und ist m ein Teiler von n, so ist $m \in E(K)$.

c) Sind $m, n \in E(K)$, so ist $\mathrm{kgV}(m,n) \in E(K)$.

Ist umgekehrt M eine Menge von natürlichen Zahlen mit den Eigenschaften a), b) und c), ist ferner p eine Primzahl, so gibt es bis auf Isomorphie genau eine algebraische Erweiterung K von $\mathrm{GF}(p)$ mit $E(K) = M$.

Die Mengen M, die die Eigenschaften a), b) und c) haben, kann man auch folgendermaßen beschreiben. Ist Π die Menge aller Primzahlen, so definieren wir durch

$$\alpha(q) := \max\{e \mid e \in \omega,\ \text{es gibt ein } n \in M \text{ mit } n \equiv 0 \bmod q^e\}$$

eine Abbildung von Π in $\omega \cup \{\infty\}$. Ist dann $n \in \omega*$, so ist genau dann $n \in M$, wenn für alle $q \in \Pi$ gilt: ist q^e ein Teiler von n, so ist $e \leq \alpha(q)$. Zu jeder algebraischen Erweiterung K von $\mathrm{GF}(p)$ gehört also eine solche Abbildung, die wir mit α_K bezeichnen. Ist $\alpha_K = \alpha_L$, so sind K und L isomorph.

9.18. Satz. *Es sei K eine algebraische Erweiterung von* $\mathrm{GF}(p)$. *Ist $\alpha_K(2) < \infty$, so gibt es ein $\gamma \in K$, so dass das Polynom $x^2 + x - \gamma$ irreduzibel ist.*

Beweis. Setze $n := 2^{\alpha_K(2)}$. Mit b) und der Definition von α_K folgt, dass K einen zu $\mathrm{GF}(p^n)$ isomorphen Teilkörper L enthält. Wir betrachten die durch

$$f(\lambda) := \lambda^2 + \lambda$$

definierte Abbildung f von L in sich. Wegen $f(0) = f(-1) = 0$ ist f nicht injektiv und folglich wegen der Endlichkeit von L auch nicht surjektiv. Es gibt also ein $\gamma \in L$ mit

$$\lambda^2 + \lambda - \gamma \neq 0$$

für alle $\lambda \in L$. Daher ist $x^2 + x - \gamma$ über L irreduzibel. Hätte dieses Polynom eine Nullstelle $\kappa \in K$, so wäre $L[\kappa]$ ein zu $\mathrm{GF}(p^{2n})$ isomorpher Teilkörper von K und es folgte der Widerspruch

$$2n = 2^{\alpha_K(2)+1} \leq 2^{\alpha_K(2)} = n.$$

Also ist $x^2 + x - \gamma$ auch über K irreduzibel.

Die Sätze 9.18 und 9.17 zeigen, dass es Quaternionenschiefkörper gibt, deren Zentrum zu $Q(Z_p)$, bzw. zu $K((x))$, dem Körper der formalen Laurentreihen über K, isomorph ist, wenn nur K eine algebraische Erweiterung eines endlichen Primkörpers ist mit $\alpha_K(2) < \infty$. Sind die Zentren zweier solcher Quaternionenschiefkörper nicht isomorph, so sind auch die fraglichen Quaternionenschiefkörper nicht isomorph, so dass die früheren Sätze zeigen, dass es Quaternionenschiefkörper wie Sand am Meer gibt. Ist H_p einer dieser Körper, so ist die durch

$$\alpha(a, b, c, d) := (a + b, -b, -c, -d)$$

definierte Abbildung α ein Antiautomorphismus von H_p.

Um zu sehen, dass es sehr viele Quaternionenschiefkörper gibt, hätte man sich nicht so anstrengen müssen. Hierauf machte mich T. Grundhöfer aufmerksam, von dem ich folgende Konstruktion lernte. Es sei Q ein Quaternionenschiefkörper — den muss man haben —. Setze $K := Z(Q)$. Schließlich sei L ein kommutativer Körper, der K, jedoch keine quadratische Erweiterung von K enthalte. Dann ist das Tensorprodukt $Q \otimes_K L$ ein Quaternionenschiefkörper mit Zentrum L. Nimmt man nun für L rein transzendente Erweiterungen von K, so erhält man sogar Quaternionenschiefkörper beliebiger Mächtigkeit.

Es gibt noch eine dritte interessante Möglichkeit, Quaternionenschiefkörper zu konstruieren. Ist nämlich K ein angeordneter Körper, so ist der Zentralisator der beiden Matrizen

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}$$

im Ring der der (4×4)-Matrizen über K ein Quaternionenschiefkörper. Dies zu beweisen, sei dem Leser als Übungsaufgabe überlassen.

10. Projektive Räume mit Clifford-Parallelismus

William Kingdon Clifford ist der Entdecker einer bemerkenswerten Eigenschaft des dreidimensionalen projektiven Raumes über dem Körper der reellen Zahlen, nämlich der Eigenschaft dieses Raumes, zwei Parallelitätsrelationen auf der Menge der Geraden zu besitzen, die beide das euklidische Parallelenpostulat erfüllen und darüber hinaus eng miteinander verknüpft sind. Ohne weitere Motivation fangen wir nun an, wie in der Mathematik üblich, das Pferd beim Schwanz aufzuzäumen.

Es sei G eine Gruppe und π sei eine Partition von G. Aus diesen Daten machen wir wie folgt eine Inzidenzstruktur $\pi(G)$. Die Punkte von $\pi(G)$ sind die Elemente von G und die Geraden die Rechtsrestklassen X_g mit $X \in \pi$ und $g \in G$. Als Inzidenz nehmen wir die Relation $\in$. Sind dann g und h zwei verschiedene Elemente von G, so ist $gh^{-1} \neq 1$, so dass es genau ein $X \in \pi$ gibt mit $gh^{-1} \in X$. Es folgt $g \in Xh$. Da auch $h \in Xh$ gilt, ist Xh eine Gerade durch die beiden Punkte g und h. Sie ist aber auch die einzige Gerade, die mit diesen beiden Punkten inzidiert. Sind nämlich g, $h \in Yf$, so gilt gf^{-1}, $hf^{-1} \in Y$ und daher $gh^{-1} = gf^{-1}(hf^{-1}) \in Y$, so dass $X = Y$ ist. dann ist aber $Xh \cap Xf \neq 0$ und folglich $Xh = Xf$. Man beachte, dass die durch

$$x^\gamma(g) := xg$$

für alle x, $g \in G$ definierte Abbildung γ ein Monomorphismus von G in die Kollineationsgruppe von $\pi(G)$ ist.

Die Partition π der Gruppe G heiße *normal*, falls für alle $X \in \pi$ und alle $g \in G$ gilt, dass auch $g^{-1}Xg \in \pi$ ist. Ist π eine normale Partition von G und ist Xg eine Gerade von $\pi(G)$, so ist $Xg = g(g^{-1}Xg)$, so dass in diesem Falle die

Menge der Geraden von $\pi(G)$ auch gleich der Menge der Linksrestklassen nach den Komponenten von π ist.

Der Satz von Dandelin, den wir im ersten Kapitel bewiesen haben, ist nicht nur schön, er ist auch nützlich, wie wir sehen werden.

10.1. Satz. *Es sei G eine Gruppe und π sei eine normale, nicht triviale Partition von G. Ist $\pi(G)$ eine irreduzible projektive Geometrie, so ist $\pi(G)$ pappossch.*

Beweis. Zunächst beachten wir, dass es in $\pi(G)$ windschiefe Geraden gibt. Ist nämlich $X \in \pi$, so ist $X \neq G$, da π nicht trivial ist. Es gibt also ein $g \in G - X$. Dann sind aber X und Xg zwei windschiefe Geraden. Hieraus folgt, dass der Rang von $\pi(G)$ mindestens gleich 4 ist.

Sind X und Y zwei verschiedene Komponenten von π, sind g_1, g_2, g_3 drei verschiedene Elemente aus $Y - \{1\}$ und h_1, h_2, h_3 drei verschiedene Elemente in $X - \{1\}$, so bilden die Geraden Xg_1, Xg_2, Xg_3 und h_1Y, h_2Y, h_3Y ein *Hexagramme mystique*. Um dies einzusehen, sei zunächst $Xg_i = Xg_k$. Dann ist

$$g_i {g_k}^{-1} \in X \cap Y = \{1\}$$

und daher $i = k$, so dass die Geraden Xg_1, Xg_2 und Xg_3 paarweise verschieden sind. Da sie verschieden sind, sind sie auch paarweise windschief. Analog sieht man dass die Geraden h_1Y, h_2Y, h_3Y — dies sind Geraden, da π normal ist —, paarweise windschief sind. Wegen

$$h_i g_k \in Xg_k \cap h_i Y$$

bilden sie also ein *Hexagramme mystique*.

Es seien nun X und Y zwei verschiedene Geraden von $\pi(G)$, die sich im Punkte s schneiden. Dann sind Xs^{-1} und Ys^{-1} zwei Geraden, die sich im Punkte 1 schneiden, so dass wir des weiteren annehmen dürfen, dass $s = 1$ ist. Dann sind aber X und Y zwei verschiedene Komponenten von π. Sind nun g_1, g_2 und g_3 drei verschiedene Punkte aus $Y - \{1\}$ und h_1, h_2 und h_3 drei verschiedene Punkte aus $X - \{1\}$, so ist Xg_1, Xg_2, Xg_3, h_1Y, h_2Y, h_3Y ein *Hexagramme mystique*, wie wir gerade gesehen haben. Nach dem Satz I.1.10 von Dandelin sind daher die Punkte

$$(g_1 + h_2) \cap (g_2 + h_1)$$
$$(g_2 + h_3) \cap (g_3 + h_2)$$
$$(g_3 + h_1) \cap (g_1 + h_3)$$

kollinear, so dass in $\pi(G)$, wie behauptet, der Satz von Pappos gilt.

Bevor wir uns auf die Suche nach Gruppen G begeben, die eine normale Partition π besitzen, so dass $\pi(G)$ eine irreduzible projektive Geometrie ist, beweisen wir einen Satz von Karzel, der die Suche erheblich erleichtert. Der hier vorgetragene Beweis stammt von mir (Karzel 1965, Lüneburg 1969a).

10.2. Satz. *Es sei G eine Gruppe und π sei eine normale, nicht triviale Partition von G. Ist $\pi(G)$ eine irreduzible projektive Geometrie, so ist G eine elementarabelsche 2-Gruppe oder es ist $\mathrm{Rg}(\pi(G)) = 4$.*

Beweis. Wir definieren die Bijektion ρ von G auf sich durch $x^\rho := x^{-1}$. Ist dann X_g eine Gerade von $\pi(G)$, so ist $(X_g)^\rho = g^{-1}X$ wegen der Normalität von π ebenfalls eine Gerade von $\pi(G)$, so dass ρ eine Kollineation von $\pi(G)$ ist. Ist $\rho = 1$, so ist G eine elementarabelsche 2-Gruppe. Es sei also $\rho \neq 1$. Dann ist ρ eine involutorische Kollineation von $\pi(G)$, die alle Geraden durch den Punkt 1 festlässt, so dass ρ eine Zentralkollineation mit dem Zentrum 1 ist. Nach Satz 1.2 besitzt ρ daher eine Achse H. Ist $x \in H$, so gilt offenbar $x^2 = 1$. Ist andererseits $y \neq 1 = y^2$, so ist y ein von 1 verschiedener Fixpunkt von ρ und daher $y \in H$.

Es sei $h \in H$ und I sei die Menge der mit h vertauschbaren Elemente aus H. Wir zeigen, dass

$$I = (H \cap Hh) \cup \{h\}$$

ist. Es sei $j \in I$ und es gelte $j \neq h$. Dann ist $jh \neq 1$ und

$$(jh)^2 = j^2h^2 = 1.$$

Daher ist nach obiger Bemerkung $jh \in H$. Ferner folgt

$$j = (jh)h \in H \cap Hh.$$

Also ist $I \subseteq (H \cap Hh) \cup \{h\}$. Ist umgekehrt $k \in (H \cap Hh) \cup \{h\}$ und ist $k \neq h$, so gibt es ein $x \in H$ mit $k = xh$. Es folgt $kh = x$ und weiter

$$1 = x^2 = (kh)^2,$$

so dass $kh = hk$ ist. Also ist $k \in I$ und obige Gleichung damit bewiesen.

Wir betrachten nun zusätzlich den Fall, dass ρ eine Elation ist. In diesem Fall hat ρ keinen Fixpunkt außerhalb H. Es gilt also

$$H = \{x \mid x \in G, x^2 = 1\}.$$

Man beachte, dass in diesem Falle jede Untergruppe von G, die in H enthalten ist, abelsch ist.

Es sei $1 \neq h \in H$ und C bezeichne den Zentralisator von h in G, dh., die Menge aller mit h vertauschbaren Elemente von G. Der Zentralisator C von h ist natürlich eine Untergruppe von G. Wir zeigen, dass C in H enthalten ist. Es sei U die Komponente von π, die h enthält. Weil U die beiden Punkte 1 und h enthält, folgt $U \subseteq H$. Es sei $g \in C$ und es gelte $g \notin U$. Es sei V die Komponente von π, die hg, und W die Komponente, die g enthält. Dann ist $V \neq W$, da sonst $h \in U \cap V = \{1\}$ wäre. Also ist

$$g^2 = h^2g^2 = (hg)^2 \in V \cap W = \{1\},$$

so dass $g \in H$ gilt. Dies zeigt, dass $C \subseteq H$ ist. Nach dem, was wir weiter oben gesehen haben, ist also $C = (H \cap Hh) \cup \{h\}$. Wegen $h = 1h$ ist aber $h \in H \cap Hh$, so dass

$$C = H \cap Hh$$

gilt.

Es sei $g \in G - H$. Dann ist $H \neq Hg$, da ja $g = 1g \in Hg$ ist. Wäre H eine Untergruppe von G, so folgte $H \cap Hg = \emptyset$ und damit, da H und Hg ja Hyperebenen sind, $\mathrm{Rg}(\pi(G)) = 2$ im Widerspruch zu $\mathrm{Rg}(\pi(G)) \geq 4$. Also ist $C \neq H$, so dass C als Schnitt von zwei Hyperebenen den KoRg-Rang 2 hat. Es sei $1 \neq d \in C$ und D sei der Zentralisator von d in G. Dann ist $C \subseteq D$, da C abelsch ist. Weil auch D ein Unterraum des Ko-Ranges 2 ist, folgt $C = D$. Es gibt nun ein $e \in H - C$. Es sei E der Zentralisator dieses Elementes. Dann ist also $C \neq E$ und folglich $C \cap E = \{1\}$, wie wir gerade gesehen haben. Damit haben wir zwei Unterräume des Ko-Ranges 2 gefunden, die sich in genau einem Punkte schneiden. Hieraus folgt, dass der Rang von $\pi(G)$ gleich 4 ist.

Es bleibt der Fall zu betrachten, dass ρ eine Streckung ist. Hier gilt

$$H = \{x \mid x \in G, x^2 = 1 \neq x\}.$$

Es sei $h \in H$ und I sei der Zentralisator von h in H. Dann ist, wie wir gesehen haben

$$I = (H \cap Hh) \cup \{h\}.$$

Ferner gilt $h \notin H \cap Hh$, da andernfalls $1 \in H$ wäre. Der Rang von $H \cap Hh$ ist mindestens 2. Es gibt also ein $b \in H \cap Hh$. Es folgt $b = ah$ mit einem $a \in H$. Es folgt $h = ab$ und damit wieder $ab = ba$. Wir betrachten den Schnitt $Ha \cap Hb$. Dann ist

$$1 = aa = bb \in Ha \cap Hb,$$

da a und b ja in H liegen. Wegen $h = ab = ba$ ist auch $h \in Ha \cap Hb$. Es sei nun $d \in Ha \cap Hb$. Es folgt da, $db \in H$. Also ist $(da)^2 = 1 = (db)^2$. Hieraus folgt $ada = d^{-1} = bdb$. Und weiter

$$hdh = abdba = ad^{-1}a = d,$$

so dass d und damit $Ha \cap Hb$ im Zentralisator von h in G liegt. Es folgt

$$Ha \cap Hb \cap H \subseteq I = (H \cap Hh) \cup \{h\}.$$

Nun ist $Ha \cap Hb \cap H$ ein Unterraum von $\pi(G)$, der h enthält. Weil h nicht in $H \cap Hh$ liegt und jede Gerade, die h mit einem Punkt von $H \cap Hh$ liegt, folgt

$$Ha \cap Hb \cap H = \{h\}.$$

Dies impliziert wieder, dass der Rang von $\pi(G)$ gleich 4 ist. Damit ist der Satz bewiesen.

Es sei π eine normale Partition der Gruppe G und $\pi(G)$ sei eine projektive Geometrie. Sind X und Y zwei Geraden von $\pi(G)$, so heißen X und Y *rechtsparallel*, falls es ein $U \in \pi$ und g, $h \in G$ gibt mit $X = Ug$ und $Y = Uh$. Die Geraden X und Y heißen *linksparallel*, falls es ein $U \in \pi$ und g, $h \in G$ gibt mit $X = gU$ und $Y = hU$. Diese beiden Parallelitätsrelationen erfüllen offensichtlich das euklidische Parallelenpostulat. Sie sind Verallgemeinerungen der

oben erwähnten cliffordschen Parallelitätsrelationen. Sie werden explizit nicht mehr auftauchen.

10.3. Satz. *Es sei π eine normale, nicht triviale Partition der Gruppe G. Ist $\pi(G)$ eine projektive Geometrie, so gilt:*

a) *Ist K eine Hyperebene von $\pi(G)$, so ist $G = K^{-1}K$. Insbesondere ist $G = HH$, wobei H wieder Achse der oben definierten Zentralkollineation ρ ist.*

b) *Ist $X \in \pi$, so ist X abelsch.*

c) *G ist eine elementarabelsche 2-Gruppe oder es ist $Z(G) = \{1\}$.*

Beweis. a) Es sei $g \in G$. Da der Rang von $\pi(G)$ mindestens 4 ist, ist der Schnitt der beiden Hyperebenen K und Kg nicht leer. Es gibt also k, $l \in K$ mit $k = lg$, so dass $g = l^{-1}k$ ist.

b) Es sei $1 \neq g \in X$. Nach a) gibt es u, $v \in H$ mit $g = uv$. Es ist $v \in Xv$ und $u = uvv = gv$. Weil $g \neq 1$ ist, ist $u \neq v$, so dass die Gerade Xv in H liegt. Daher ist $(xv)^2 = 1$ und damit $vxv = x^{-1}$ für alle $x \in X$. Hieraus folgt

$$vxyv = (xy)^{-1} = y^{-1}x^{-1} = vyvvxv = vyxv$$

und dann $xy = yx$ für alle x, $y \in X$, so dass X abelsch ist.

c) Es sei u eine Involution von G und v sei ein mit u vertauschbares Element von G. Dann liegen u und v entweder in der gleichen Komponente von π oder aber es ist $v^2 = 1$. Sind nämlich V, $W \in \pi$ und gilt $v \in V$ und $uv \in W$, so ist $V \neq W$ und daher

$$v^2 = (uv)^2 \in V \cap W = \{1\}.$$

(Dieser Schluss wurde nun schon so häufig gezogen, dass er es eigentlich verdient hätte, als Hilfssatz formuliert zu werden.)

Ist nun $1 \neq g \in Z(G)$, so gibt es eine Involution in G, die nicht in der gleichen Komponente wie g liegt. Nach der Vorbemerkung ist also $g^2 = 1$, so dass $Z(g)$ eine elementarabelsche 2-Gruppe ist. Wäre nun ρ nicht die Identität, so läge $Z(G) - \{1\}$ in der Achse H von ρ und die Elemente außerhalb H hätten nicht die Ordnung 2 im Widerspruch zu unserer Vorbemerkung.

Wir ziehen nun einige interessante Folgerungen aus Satz 10.2. Zunächst eine geometrische, die wir durch den folgenden Satz vorbereiten.

10.4. Satz. *Es sei G eine Gruppe und U eine Teilmenge von G mit $|U - \{1\}| \geq 2$. Gilt dann $U^{-1}x = U$ für alle von 1 verschiedenen $x \in U$, so ist U eine Untergruppe von G.*

Beweis. Es sei $H := \{g \mid g \in G,\ Ug = U\}$. Dann ist H eine Untergruppe von G. Es sei $u \in U$. Es gibt dann ein $v \in U$ mit $v \neq 1$, u. Es folgt $U = U^{-1}v$. Es gibt daher ein $x \in U$ mit $u = x^{-1}v$. Wegen $u \neq v$ ist $x \neq 1$ und daher $U = U^{-1}x$. Somit ist $U^{-1} = Ux^{-1}$. Es folgt

$$U = U^{-1}v = Ux^{-1}v = Uu$$

und weiter $u \in H$. Es ist also $U \subseteq H$. Weil H eine Gruppe ist, folgt $U^{-1} \subseteq H$. Aus der Definition von H folgt schließlich $UU^{-1} \subseteq U$. Dies zeigt, dass U eine Untergruppe von G ist.

10.5. Satz. *Es sei G eine Gruppe und die Elemente von G seien gleichzeitig die Punkte einer irreduziblen projektiven Geometrie $\Lambda(G)$ mit $\mathrm{Rg}(\Lambda(G)) \geq 3$. Für alle $g \in G$ sei die durch $x^{\kappa(g)} := xg$ definierte Abbildung $\kappa(g)$ von G in sich eine Kollineation von $\Lambda(G)$. Ist dann auch die durch $x^\rho := x^{-1}$ definierte Abbildung ρ eine Kollineation von $\Lambda(G)$, so ist die Menge π der Geraden durch den Punkt* 1 *— die Geraden als Punktmengen aufgefasst — eine normale Partition von G, und $\pi(G)$ ist die Geometrie aus den Punkten und Geraden von $\Lambda(G)$. Insbesondere ist G also eine elementarabelsche* 2*-Gruppe oder aber es ist* $\mathrm{Rg}(\Lambda(G)) = 4$.

Beweis. Ist $U \in \pi$, so ist $|U - \{1\}| \geq 2$, da die Geraden einer irreduziblen projektiven Geometrie mindestens drei Punkte tragen. Ferner folgt, da ρ eine Kollineation ist, dass auch $U^{-1} \in \pi$ gilt. Es sei $1, x \in U$. Dann ist $1, x^{-1} \in U^{-1}x$ eine Gerade durch die Punkte x und 1. Da auch U eine Gerade durch diese beiden Punkte ist, folgt $U^{-1}x = U$. Nach 10.4 ist U daher eine Untergruppe von G, so dass π eine Partition von G ist, da jeder von 1 verschiedene Punkt von $\Lambda(G)$ auf genau einer Geraden durch 1 liegt. Diese Partition ist wegen $\mathrm{Rg}(\Lambda(G)) \geq 3$ nicht trivial. Wegen $gx = x^{\rho\kappa(g^{-1})\rho}$ ist die Abbildung $x \to gx$ ebenfalls eine Kollineation von $\Lambda(G)$. Hieraus folgt $g^{-1}Ug \in \pi$ für alle $U \in \pi$. somit ist π eine normale Partition von G. Weil die Gruppe der Kollineationen $\kappa(g)$ auf der Menge der Punkte von $\Lambda(G)$ transitiv operiert, folgt schließlich, dass $\pi(G)$ die Geometrie aus den Punkten und Geraden von $\Lambda(G)$ ist. Die restlichen Behauptungen folgen nun aus 10.2.

Die weiteren Folgerungen sind algebraischer Natur, so dass die Geometrie auch einmal anderen Teilen der Mathematik dient, was selten genug vorkommt, wie schon zu Beginn von Abschnitt 4 des Kapitels I bemerkt wurde.

10.6. Satz. *Es sei M ein Körper und K sei ein in $Z(M)$ enthaltener Teilkörper von M. Hat jedes $a \in M - K$ ein Minimalpolynom des Grades* 2 *über K, so gilt eine der folgenden Aussagen:*

a) *Es ist $K = M$.*

b) *Es ist $[M : K] = 2$.*

c) *Es ist $Z(M) = K$ und M ist ein Quaternionenschiefkörper über K.*

d) *Der Körper M ist kommutativ, die Charakteristik von M ist* 2 *und M ist eine rein inseparable Erweiterung von K mit $a^2 \in K$ für alle $a \in M$.*

Beweis. Ist $[M : K] \leq 2$, so liegt einer der beiden Fälle a) oder b) vor. Es sei also $[M : K] \geq 3$. Setze $G := M^*/K^*$. Da K im Zentrum von M liegt, ist K^* ein Normalteiler von M^*, so dass G eine Gruppe ist. Die Elemente von G sind die Restklassen mK^* mit $m \in M^*$, so dass die durch $\varphi(mK) := mK^*$ definierte Abbildung φ eine Bijektion der Menge der Punkte von $\mathrm{L}_K(M)$ auf G ist.

Es sei X eine Gerade von $L_K(M)$ durch den Punkt K. Ferner sei $a \in X - K$. Dann ist $X = K + Ka$. Weil das Minimalpolynom von a über K den Grad 2 hat, ist X ein Körper. Ist umgekehrt Y eine in M liegende, quadratische Erweiterung von K, so ist Y eine durch K gehende Gerade von $L_K(M)$. Es folgt, dass die Menge der Punkte einer Geraden durch K unter φ auf die Menge Y^*/K^*

abgebildet wird, wobei Y der Körper ist, der die fragliche Gerade repräsentiert. Es folgt, dass die Menge π der Gruppen Y^*/K^*, wobei Y eine in M liegende quadratische Erweiterung von K ist, eine Partition von G ist. Die Partition π ist aber auch normal, da innere Automorphismen von M quadratische Erweiterungen von K auf ebensolche abbilden. Sind nun aK und bK zwei Punkte von $\mathrm{L}_K(M)$, so wird durch $x^\sigma := xa^{-1}b$, da K im Zentrum von M liegt, eine bijektive lineare Abbildung von M auf sich definiert mit $(aK)^\sigma = bK$. Dies können wir so interpretieren, dass G auf der Menge der Punkte von $\mathrm{L}_K(M)$ transitiv operiert. Aus all dem folgt nun, dass $\pi(G)$ eine Beschreibung der Inzidenzstruktur aus den Punkten und Geraden von $L_K(M)$ ist. Mit Satz 10.2 erhalten wir daher, dass G eine elementarabelsche 2-Gruppe oder dass $\mathrm{Rg}(\pi(G)) = 4$ ist.

Es sei G keine elementarabelsche 2-Gruppe. Dann ist $Z(G) = \{1\}$ nach 10.3. Hieraus folgt $Z(M) = K$, so dass M ein Quaternionenschiefkörper über K ist.

Es sei G eine elementarabelsche 2-Gruppe. Dann ist $a^2 \in K$ für alle $a \in M$. Ist $a \in M - K$, so ist also

$$2a = (a+1)^2 - a^2 - 1 \in K.$$

Dies impliziert, dass die Charakteristik von M gleich 2 ist, da wegen $2 \in K$ sonst $a \in 2^{-1}K = K$ wäre. Es seien $a, b \in M^*$. Weil G abelsch ist, ist $b^{-1}ab \in K[a]$. Es gibt also $k, l \in K$ mit $b^{-1}ab = k + la$. Hieraus folgt $aba^{-1} = kba^{-1} + lb$. Andererseits ist natürlich auch $aba^{-1} \in K[b]$. Es folgt $kba^{-1} \in K[b]$. Ist $a \in K[b]$, so ist $ab = ba$. Es sei also $a \notin K[b]$. Dann ist $k = 0$ und somit $b^{-1}ab = la$. hieraus folgt, da $a^2 \in K$ gilt,

$$a^2 = b^{-1}a^2b = l^2a^2.$$

Da die Charakteristik 2 ist, impliziert dies $l = 1$. Also gilt auch in diesem Falle $ab = ba$, so dass M als kommutativ erkannt ist. Damit ist alles bewiesen.

Man beachte, dass im Fall d) der Rang von M über K eine Potenz von 2 ist, falls er endlich ist.

Der Beweis von 10.6 zeigt, wie man sich Gruppen G mit einer Partition π verschaffen kann, so dass $\pi(G)$ eine projektive Geometrie ist. Eine nähere Analyse zeigt, dass dies bereits alle Beispiele sind. Diese Analyse werden wir jedoch nicht durchführen. Der an ihr interessierte Leser sei an Karzel 1965 verwiesen.

Wir zeigen eine weitere Folgerung aus den bisherigen Entwicklungen, die sich auf Quaternionenschiefkörper der Charakteristik 2 bezieht. Sie ist Spezialfall eines viel allgemeineren Satzes. Da wir sie hier jedoch gratis bekommen, — *for love*, wie es im Englischen so poetisch heißt, — wollen wir sie hier formulieren.

10.7. Korollar. *Es sei M ein Quaternionenschiefkörper über K und die Charakteristik von M sei* 2. *Setze*

$$H := \{a \mid a \in M, a^2 \in K\}.$$

Dann ist H eine Hyperebene des K-Vektorraumes M.

a) *Für $a \in H - K$ ist $K[a]$ eine inseparable Erweiterung des Grades 2 von K.*
b) *Für $a \in M - H$ ist $K[a]$ eine separable Erweiterung des Grades 2 von K.*
M enthält also sowohl inseparable als auch separable Erweiterungen des Grades 2 von K.

Beweis. Setze $G := M^*/K^*$ und π sei die im Beweis von 10.6 beschriebene Partition von G. Weil M nicht kommutativ ist, ist G nach 10.6 keine elementarabelsche 2-Gruppe. Also ist die $g^\rho := g^{-1}$ definierte Abbildung ρ eine involutorische Perspektivität von $\pi(G)$. Weil die Charakteristik von K gleich 2 ist, können die Streckungsgruppen von $\pi(G)$, da sie zu K^* isomorph sind, keine Involutionen enthalten. Also ist ρ eine Elation. Daher gilt für die Achse A von ρ die Gleichung

$$A = \{g \mid g \in G,\ g^2 = 1\}.$$

Der im Satz definierte Unterraum H des K-Vektorraumes M ist offenbar der A entsprechende Unterraum von M.

Ist $a \in H - K$, so ist $a^2 \in K$, so dass $K[a]$ eine inseparable Erweiterung von K ist. Ist $b \in M - H$, so ist $b^2 \notin K$, so dass $K[b]$ eine separable Erweiterung von K ist. Damit ist alles bewiesen.

Es sei K ein angeordneter, kommutativer Körper. Wir nennen K *reell abgeschlossen*, falls jedes Polynom ungeraden Grades über K eine Nullstelle in K hat. Prominentestes Beispiel eines reell abgeschlossenen Körpers ist der Körper der reellen Zahlen. Der zweite Beweis, den Gauß für den Fundamentalsatz der Algebra gab, lässt sich auf reell abgeschlossene Körper übertragen, so dass also

$$K[x]/(x^2 + 1)K[x]$$

algebraisch abgeschlossen ist, falls nur K reell abgeschlossen ist. In einem reell abgeschlossenen Körper ist jedes positive Element ein Quadrat, so dass reell abgeschlossene Körper nur eine Anordnung besitzen.

Ferner haben alle über K irreduziblen Polynome den Grad 1 oder 2. Dies ist der Schlüssel zum Beweise des folgenden Satzes, der für den Fall des Körpers der reellen Zahlen von Frobenius stammt (Frobenius 1877).

10.8. Satz. *Es sei M ein Körper und K sei ein reell abgeschlossener Körper mit $K \subseteq Z(M)$. Ist dann $[M : K] < \infty$, so gilt einer der folgenden Fälle:*
a) *Es ist $M = K$.*
b) *M ist der algebraische Abschluss von K.*
c) *M ist der bis auf Isomorphie eindeutig bestimmte Quaternionenschiefkörper über K.*

Beweis. Da ein angeordneter Körper die Charakteristik 0 hat, folgt mit 10.6, dass $[M : K] = 1$, 2 oder 4 ist, da irreduzible Polynome über K ja den Grad 1 oder 2 haben. Im ersten Fall ist $M = K$. Im zweiten Fall folgt aus dem oben Referierten, dass M der algebraische Abschluß von K ist. Es gelte also $[M : K] = 4$. Dann ist M ein Quaternionenschiefkörper über K. Es bleibt zu zeigen, dass M bis aus Isomorphie eindeutig bestimmt ist.

Es sei H die Vereinigung über alle aK mit $a \notin K$ und $a^2 \in K$. Die schon verschiedentlich benutzte Perspektivität ρ zeigt, dass H eine Hyperebene des

K-Vektorraumes M ist. Ist $a \notin K$ und $a^2 \in K$, so ist das Polynom $x^2 - a^2$ über K irreduzibel. Weil K reell abgeschlossen ist, folgt hieraus

$$a^2 = -k^2$$

mit einem positiven $k \in K$. Setzt man $b := k^{-1}a$, so folgt $bK = aK$ und $b^2 = -1$. Hieraus folgt

$$H = \bigcup_{b \in M,\ b^2+1=0} bK.$$

(An dieser Stelle sieht man sehr schön, dass es die Kommutativität ist, die erzwingt, dass ein Polynom über einem kommutativen Körper höchstens so viele Nullstellen besitzt, wie der Grad des Polynoms angibt, da im vorliegenden Falle das Polynom $x^2 + 1$ ja unendlich viele Nullstellen hat.)

Es sei $i \in H$ und es gelte $b^2 = -1$. Ist $ib = -bi$, so setzen wir $j := b$. Es sei $ib \neq -bi$. Wegen

$$ib + bi = (i + b)^2 - i^2 - b^2$$

ist $ib + bi \in K$. Wir machen nun nach dem Vorgang von Fibonacci den falschen Ansatz $\lambda := ib + bi$ und $\mu := 2$, der uns dann doch zum rechten Ziele führt. Mit diesem Ansatz folgt

$$i(\lambda i + \mu b) + (\lambda i + \mu b)i = -2\lambda + \mu(ib + bi) = 0.$$

Weil λ und μ nicht Null und i und b linear unabhängig sind, ist $(\lambda i + \mu b)K$ ein von iK verschiedener Punkt in H. Wie wir oben gesehen haben, gibt es ein $j \in (\lambda i + \mu b)K$ mit $j^2 = -1$. Es folgt, dass $ij = -ji$ ist. Es folgt weiter

$$(ij)^2 = ijij = -jiij = (-1)^3 = -1$$

und damit $j \in K[i] \cap H = iK$. Dieser Widerspruch zeigt, dass i, j, ij eine Basis von H ist. Folglich ist 1, i, j, ij eine Basis von M. Hieraus folgt alles Weitere.

Der Beweis des letzten Satzes zeigt auch, dass es über einem angeordneten Körper, dessen positive Elemente allesamt Quadrate sind, bis auf Isomorphie nur einen Quaternionenschiefkörper gibt.

Nach Satz 8.1 ist $L(V)$ genau dann selbstdual, wenn der Rang von V endlich ist und wenn außerdem der $L(V)$ zu Grunde liegende Koordinatenkörper einen Antiautomorphismus gestattet. Daher ist es interessant, auch nicht kommutative Körper zu kennen, die einen Antiautomorphismus besitzen. Es ist nun nicht schwer zu sehen, dass alle von uns konstruierten Quaternionenschiefkörper einen involutorischen Antiautomorphismus haben. Wir werden zeigen, dass sogar alle Quaternionenschiefkörper einen solchen besitzen. Dazu beweisen wir zunächst:

10.9. Satz. *Ist M ein Quaternionenschiefkörper über K, so gibt es Elemente i, j, $k \in M$ und Elemente γ, $\delta \in K$, so dass 1, i, j, k eine Basis des K-*

Vektorraumes M ist und die folgenden Relationen gelten:

$$\begin{aligned} i^2 &= i + \gamma, \\ ij &= k, \\ ik &= k + \gamma j, \\ ji &= j - k, \\ j^2 &= \delta, \\ jk &= \delta - \delta i, \\ ki &= -\gamma j, \\ kj &= \delta i, \\ k^2 &= -\gamma\delta. \end{aligned}$$

Beweis. Wir beginnen den Beweis mit der folgenden Bemerkung. Sind u, $v \in M$, so ist $u^2 \in Ku + K$ und $v^2 \in Kv + K$ sowie $(u+v)^2 \in K(u+v) + K$. Hieraus folgt, dass

$$uv + vu \in Ku + Kv + K$$

ist.

Wäre $x^2 \in K$ für alle $x \in M$, so wäre M^*/K^* eine elementarabelsche 2-Gruppe. Wie der Beweis von 10.6 zeigt, wäre M ein kommutativer Körper im Widerspruch zu unserer Voraussetzung. Es gibt also ein $y \in M$ mit $y^2 \notin K$. Es gibt somit Elemente r, $s \in K$ mit $r \neq 0$ und $y^2 = ry = ry + s$. Setze $i := yr^{-1}$ und $\gamma := sr^{-2}$. Dann ist

$$i^2 = y^2 r^{-1} = (ry + s)r^{-2} = i + \gamma.$$

$Ki + K$ ist ein kommutativer Teilkörper von M. Es gibt folglich ein $z \in M$, welches nicht in $Ki + K$ liegt. Nach der eingangs gemachten Bemerkung gibt es r, s, $t \in K$ mit

$$iz + zi = ri + sz + t.$$

Es gibt ferner ein $u \in K$ mit $z^2 - uz \in K$. Sind l, $m \in K$, so folgt

$$\begin{aligned} &-(li + mz)^2 + (l + mr)li + (mu + ls)mz \\ &\qquad = -l^2(i^2 - i) - m^2(z^2 - uz) - ml(iz + zi - ri - sz). \end{aligned}$$

Dies zeigt, dass

$$-(li + mz)^2 + (l + mr)li + (mu + ls)mz \in K$$

ist. Es gibt auch ein $v \in K$ mit

$$(li + mz)^2 - v(li + mz) \in K.$$

Aus diesen beiden Gleichungen folgt

$$(l + mr - v)li + (mu + ls - v)mz \in K.$$

Weil 1, i, y über K linear unabhängig sind, folgt

$$(l + mr - v)l = 0 = (mu + ls - v)m.$$

Letztere Gleichung gilt für alle l, $m \in K$, da l und m ja irgendwelche Elemente von K waren. Wählt man insbesondere l und m in K^*, so folgt

$$l + mr = v = mu + ls.$$

Dies hat wiederum

$$l(1 - s) = m(r - u)$$

zur Folge. Mit $l = m = 1$ folgt

$$1 - s = r - u.$$

Weil K das Zentrum von M ist, ist K nicht endlich. Es gibt also ein $l \in K^* - \{1\}$. Mit $m = 1$ folgt

$$l(1 - s) = r - u = 1 - s,$$

so dass $s - 1 = 0$ und daher $s = 1$ und $r = u$ ist. Also ist

$$iz + zi = ri + z + t$$

und

$$z^2 - rz \in K.$$

In (1) ist $4\gamma + 1 \neq 0$, sonst wäre nämlich

$$(2i - 1)^2 = 4i^2 - 4i + 1 = 4(i + \gamma) - 4i + 1 = 0$$

und folglich $2i - 1 = 0$. Dies hätte $2 \neq 0$ und dann den Widerspruch $i \in K$ zur Folge. Wir setzen nun

$$j := z - (r + 2t)(4\gamma + 1)^{-1}i + (t - 2r\gamma)(4\gamma + 1)^{-1}.$$

Unter Benutzung von (2) und (1) erhält man nach einfacher Rechnung

$$ij + ji = j.$$

Drückt man nun z gemäß (4) durch i und j aus und berechnet $z^2 - rz$, so erhält man unter Benutzung von (5) und (1), dass die Koeffizienten bei j und i Null sind, dh., man erhält eine Gleichung der Form

$$z^2 - z = y^2 + w$$

mit einem $w \in K$. Setzt man $\delta := z^2 - z - w$, so folgt mit (5), dass $\delta \in K$ gilt.

Wäre $ij \in Ki + Kj + K$, so gäbe es u, v, $w \in K$ mit $ij = ai + vj + w$. Es folgte

$$(i - v)j = ai + w \in Ki + K.$$

Wegen $j \notin K$ folgte $i - v = 0$ und damit der Widerspruch $i \in K$. Dies zeigt, dass 1, i, j, ij eine Basis von M über K ist. Setze $k := ij$. Es gilt nun, die neun Relationen des Satzes herzuleiten. Die erste ist bereits nachgewiesen und die zweite ist Inhalt der Definition von k. Es ist

$$ik = i^2 j = (i + \gamma)j = k + \gamma j.$$

Mit (5) folgt

$$ji = j - ij = j - k.$$

Dass $j^2 = \delta$ ein Element von K ist, wurde dem Leser überlassen nachzurechnen. Es ist

$$jk = jij = (j - ij)j = j^2 - ij^2 = \delta - \delta i,$$

da d ja im Zentrum K von M liegt. Weiter ist

$$ki = iji = i(j - ij) = ij - (i + \gamma)j) = -\gamma j$$

und

$$kj = ij^2 = \delta i.$$

Schließlich ist

$$k^2 = ijij = i(j - ij)j = i(\delta - i\delta) = i\delta - (i + \gamma)\delta = -\gamma\delta.$$

Damit ist alles bewiesen.

Mittels der in 10.9 notierten Relationen verifiziert man, dass Folgendes gilt: Ist

$$(a + bi + cj + dk)(a' + b'i + c'j + d'k) = a'' + b''i + c''j + d''k,$$

so ist

$$\begin{aligned} a'' &= aa' + bb'\gamma + cc'\delta + cd'\delta - dd'\gamma\delta \\ b'' &= ab' + ba' + bb' - cd'\delta + dc'\delta \\ c'' &= ac' + ca' + bd'\gamma + cb' - db'\gamma \\ d'' &= ad' + da' + bc' + bd' - cb'. \end{aligned}$$

10.10. Satz. *Es sei M ein Quaternionenschiefkörper über K und* 1, i, j, k *sei die in 10.9 beschriebene K-Basis von M. Ist $x = z + ui + vj + wk$ mit z, u, v, $w \in K$ und setzt man*

$$x^\alpha := z + u - (ui + vj + wk),$$

so ist α ein involutorischer Antiautomorphismus von M.

Ist $\mathrm{Char}(K) \neq 2$*, so sind die Fixelemente von α genau die Elemente von K. Ist* $\mathrm{Char}(K) = 2$*, so sind die Fixelemente von α genau die Elemente mit $u = 0$.*

Beweis. Dass α involutorisch ist, ist unmittelbar zu sehen. Ebenfalls, dass $(x+y)\alpha = x^\alpha + y^\alpha$ ist. Ebenso ist die Aussage über die Fixelemente von α wegen der linearen Unabhängigkeit von 1, i, j, k banal. Das einzige, nicht triviale, was

nachzuweisen ist, ist, dass $(xy)^\alpha = y^\alpha x^\alpha$ ist. Dazu berechne man mittels der vor Satz 10.10 aufgelisteten Relationen für x, $y \in M$ einmal $(xy)^\alpha$ und zum anderen $y^\alpha x^\alpha$, um herauszufinden, dass die beiden Ergebnisse übereinstimmen.

Ist M ein Quaternionenschiefkörper der Charakteristik 2, so bilden die Fixelemente des in Satz 10.10 beschriebene Antiautomorphismus α einen Unterraum des Ranges 3 des $Z(M)$-Vektorraumes M. Daher wird M als Körper von diesen Fixelementen erzeugt. Ist die Charakteristik von M von 2 verschieden, so machen die Fixelemente von α gerade das Zentrum von M aus. Diese Situation ist typisch für Quaternionenschiefkörper mit von 2 verschiedener Charakteristik, wie der nächste, von Dieudonn stammende Satz zeigt.

10.11. Satz. *Es sei K ein Körper und α sei ein Antiautomorphismus von K mit $\alpha^2 = 1$. Setze*

$$L := \{x \mid x \in K, x^\alpha = x\}.$$

Dann gilt einer der folgenden Fälle.

a) *Der Körper K ist kommutativ, L ist ein Teilkörper von K und $[K : L] \leq 2$.*

b) *L ist das Zentrum von K und K ist ein Quaternionenschiefkörper über L mit von 2 verschiedener Charakteristik.*

c) *K wird von L erzeugt.*

Beweis. Ist K kommutativ, so ist α ein Antiautomorphismus von K. In diesem Falle ist L ein Teilkörper von K und es gilt nach bekannten Sätzen, dass der Grad von K über L höchstens 2 ist, dh., es gilt a).

Es sei des Weiteren K nicht kommutativ. Wir nehmen zunächst an, dass $L \subseteq Z(K)$ gelte. Dann ist L ein Teilkörper von $Z(K)$. Wegen

$$(k + k^\alpha)^\alpha = k^\alpha + k^{\alpha^2} = k + k^\alpha$$

und

$$(k^\alpha k)^\alpha = k^\alpha + k^{\alpha^2} = k^\alpha k$$

ist

$$k + k^\alpha,\ k^\alpha k \in L$$

für alle $k \in K$. Nun ist

$$k^2 - (k + k^\alpha)k + k^\alpha k = 0$$

für alle $k \in K$. Nach 10.6 ist daher K ein Quaternionenschiefkörper über L, da wir K als nicht kommutativ vorausgesetzt hatten. Es bleibt zu zeigen, dass die Charakteristik von K nicht 2 ist.

Wir nehmen an, dass die Charakteristik von K gleich 2 sei. Setze

$$H := \{a \mid a \in K,\ a^2 \in K\}.$$

Dann ist H nach 10.7 eine Hyperebene des $Z(K)$-Vektorraumes K. Offenbar wird H von α invariant gelassen und α induziert eine semilineare Abbildung

auf dem $Z(K)$-Vektorraum H. Es sei $0 \neq a \in H$. Dann ist $a^2 \in Z(K)$ und andererseits auch $aa^\alpha \in L \subseteq Z(K)$. Es folgt

$$a^{-1}a^\alpha = a^{-2}aa^\alpha \in Z(K).$$

Dies besagt, dass α alle Punkte von H festlässt. Nach Satz III.1.2 gibt es daher ein $k \in Z(K)$ mit $h^\alpha = hk$ für alle $h \in H$. Insbesondere ist dann $1 = 1^\alpha = k$. Folglich ist $h^\alpha = h$ für alle $h \in H$ im Widerspruch zu unserer Annahme, dass $L \subseteq Z(K)$ gilt. Also gilt auch b).

Es bleibt der Fall zu betrachten, dass $L \not\subseteq Z(K)$ gilt. Es sei R der von L erzeugte Teilring von K. Ist $0 \neq r \in R$, so ist auch $r^\alpha \in R$. Setze $d := rr^\alpha$. Dann ist $0 \neq d \in L$. Folglich ist auch $d^{-1} \in L \subseteq R$. Dann ist aber auch

$$r^{-1} = r^\alpha d^{-1} \in R,$$

so dass R sogar ein Körper ist. Wir wollen zeigen, dass $R = K$ ist. Dazu nehmen wir an, dass dies nicht der Fall sei. Es sei $a \in K - R$. Es sei $u \in R$. Dann ist

$$au + u^\alpha a^\alpha = au + (au)^\alpha \in L.$$

Es folgt

$$au - u^\alpha a = au + u^\alpha a^\alpha - u^\alpha(a + a^\alpha) \in R.$$

Andererseits ist auch

$$u^\alpha a - au^\alpha = u^\alpha a + a^\alpha u - (a^\alpha + a)u^\alpha \in R.$$

Somit ist schließlich $a(u - u^\alpha) \in R$. Weil a nicht in R liegt, folgt $u^\alpha = u$. Somit ist $R \subseteq L$ und damit $R = L$, so dass L ein Körper ist. Sind u, $v \in L$, so ist auch $uv \in L$ und es gilt

$$uv = (uv)^\alpha = v^\alpha u^\alpha = vu,$$

so dass L ein kommutativer Körper ist.

Durch $D(u) := au - u^\alpha a$ wird, wie schon gesehen, eine Abbildung von R in sich definiert. Weil $R = L$ ist, ist also

$$D(u) = au - ua.$$

Es sei zunächst $\mathrm{Char}(K) \neq 2$. Dann ist

$$a = \tfrac{1}{2}(a + a^\alpha) + \tfrac{1}{2}(a - a^\alpha).$$

Das Element $a - a^\alpha$ ist nicht in R. Wir können daher a durch $a - a^\alpha$ ersetzen. Es ist dann $a^\alpha = -a$ und demzufolge $a^2 = -aa^\alpha \in R$. Es ist

$$D^2(u) = a(au - ua) - au - ua)a = a^2u - 2aua + ua^2 \in R.$$

Wegen $a^2u \in R$ ist daher $aD(u) \in R$. Weil R ein Körper ist und a nicht in R liegt, ist daher $D(u) = 0$, so dass $au = ua$ ist. Dies zeigt, dass jedes $u \in R$ mit jedem $a \in K$ vertauschbar ist, für das $a^\alpha = -a$ ist. Nun ist aber

$$a = \tfrac{1}{2}(a + a^\alpha) + \tfrac{1}{2}(a - a^\alpha),$$

so dass a die Summe eines Elementes $b \in R$ und einem Element c mit $c^\alpha = -c$ ist. Weil R kommutativ ist, ist daher jedes $u \in R$ mit allen $a \in K$ vertauschbar. Also liegt R und damit L im Zentrum von K im Gegensatz zu unserer Annahme.

Es bleibt der Fall zu betrachten, dass $\mathrm{Char}(K) = 2$ ist. Es sei wieder $a \in K - R$. Setze

$$V := aR + R.$$

Dann ist V ein Rechtsvektorraum über R. Wir zeigen, dass V ein Teilkörper von K ist. Dazu ist zu zeigen, dass V multiplikativ abgeschlossen ist und dass das Inverse eines von Null verschiedenen Elementes aus V wieder zu V gehört. Es ist

$$a^2 = a(a + a^\alpha) - aa^\alpha$$

und $a + a^\alpha$, $aa^\alpha \in R$, so dass $a^2 \in V$ gilt.

Als Nächstes zeigen wir, dass auch $ra \in V$ ist für alle $r \in R$. Dazu dürfen wir natürlich annehmen, dass $r \neq 0$ ist. Von den im Folgenden zu betrachtenden Elementen aus L nehmen wir an, dass sie von Null verschieden sind. Es sei $u \in L$. Dann ist

$$au + ua^\alpha = au + (au)^\alpha \in L.$$

Hieraus folgt weiter

$$au - ua = au + ua^\alpha - u(a + a^\alpha) \in R.$$

Es sei $n > 1$, es seien $u_1, \ldots, u_n \in L$ und es gelte

$$au_1 \cdots u_{n-1} - u_1 \cdots u_{n-1}a \in V.$$

Weil die u_i allesamt als von Null verschieden angenommen sind, ist $aR = au_1 \cdots u_{n-1}R$. Wir können und werden daher in dem vorangegangenen Argument a durch $au_1 \cdots u_{n-1}$ ersetzen. Man erhält dann, dass

$$au_1 \cdots u_n - u_n u_1 \cdots u_{n-1}a \in V.$$

liegt. Weil R kommutativ ist, folgt weiter, dass auch

$$au_1 \cdots u_n - u_1 \cdots u_n a \in V$$

liegt. Da R als Ring additiv abgeschlossen ist, folgt schließlich, dass

$$ar - ra \in V$$

für alle $r \in R$ gilt. Dies impliziert wiederum, dass $ra \in V$ ist für alle $r \in R$. Weiter folgt, dass

$$\begin{aligned}(ar + s)(ar' + s') &= arar' + ars' + sar' + ss' \\ &= a^2rr' + at + t'\end{aligned}$$

ist mit t, $t' \in R$. Weil $a^2 \in V$ ist, folgt, dass V multiplikativ abgeschlossen ist.

Es ist $a + a^\alpha \in L = R$. Hieraus folgt, dass

$$a^\alpha \in aR + R = V$$

ist. Es folgt weiter, dass $x^\alpha \in V$ ist für alle $x \in V$. Ist nun $0 \neq x \in V$, so ist $d := xx^\alpha \in L$. Dann ist auch $d^{-1} \in L$ und folglich $x^{-1} = x^\alpha d^{-1} \in V$. Damit ist gezeigt, dass V ein Körper ist.

Es gilt

$$a(a + a^\alpha)a + aa^\alpha a = a^3 = a^2(a + a^\alpha) + a^2 a^\alpha.$$

Also ist

$$aD(a + a^\alpha) = D(aa^\alpha) \in R.$$

Hieraus folgt $D(a + a^\alpha) = 0$ und dann auch $D(aa^\alpha) = 0$, so dass a mit $a + a^\alpha$ und aa^α vertauschbar ist. Setze $b := a + a^\alpha$ und $c := aa^\alpha$. Dann ist

$$(ab^{-1})^2 = a^2 b^{-2} = (ab + c)b^{-2} = ab^{-1} + cb^{-2}.$$

Ersetzt man a durch ab^{-1}, so ist also $a + a^\alpha = 1$ und daher

$$a^2 = a + aa^\alpha.$$

Überdies ist a mit aa^α vertauschbar und es gilt nach wie vor $V = aR + R$.

Es sei Z der Zentralisator von a in R. Weil R kommutativ ist, liegt Z im Zentrum von V. Es sei $x \in R$. Dann ist wegen $a^2 = a + aa^\alpha$ und $aa^\alpha \in R$ und weil die Charakteristik ja 2 ist,

$$\begin{aligned} D^2(x) &= D(ax - xa) \\ &= a^2 x - axa - axa + xa^2 \\ &= (a + aa^\alpha)x + x(a + aa^\alpha) \\ &= D(x) \end{aligned}$$

für alle $x \in R$. Also ist

$$D\bigl(D(x) + x\bigr) = 0,$$

so dass $D(x) + x \in Z$ gilt für alle $x \in R$. Hieraus folgt

$$D(x)x - xD(x) = \bigl(D(x) + x\bigr)x - x\bigl(D(x) + x\bigr) = 0.$$

Weiter folgt

$$D(x^2) = D(x^2) - 2xD(x) = D(x)x - xD(x) = 0.$$

Also ist $x^2 \in Z$ für alle $x \in R$. Es sei $u \in V$. Dann ist $u = ar + s$ mit $r,s \in R$. Es folgt, da $r^2 \in Z$ und $a + a^\alpha = 1$ ist,

$$\begin{aligned} uu^\alpha &= (ar + s)(ra^\alpha + s) \\ &= ar^2 a^\alpha + ars + sra^\alpha + s^2 \\ &= aa^\alpha r^2 + D(rs) + rs(a + a^\alpha) + s^2 \\ &= aa^\alpha r^2 + D(rs) + rs + s^2. \end{aligned}$$

Wir haben schon gesehen, dass aa^α mit a vertauschbar ist. Da aa^α auch in R liegt, ist aa^α ein Element von Z. Weil auch r^2, s^2 und $D(rs) + rs$ in Z liegen, ist uu^α für alle $u \in V$ ein Element von Z. Weiter gilt

$$u + u^\alpha = ar + s + ra^\alpha + s = ar + ra + r(a + a^\alpha) = D(r) + r,$$

so dass auch $u + u^\alpha$ für alle $u \in V$ ein Element von Z ist. Wegen

$$u^2 + u(u + u^\alpha) + uu^\alpha = 0$$

haben wir für V und Z die in Satz 10.6 beschriebene Situation.

Wir nehmen zunächst an, V sei ein Quaternionenschiefkörper über Z. Es ist $uu^\alpha \in Z$ für alle $u \in V$. Ist $u \neq 0$, so folgt $u^{-1}Z^* = u^\alpha Z^*$, so dass die Kollineation $uZ^* \to u^{-1}Z^*$ durch die Z-lineare Abbildung α induziert wird. Diese Kollineation ist aber eine Elation, wie wir schon früher bemerkten. Daher lässt α eine Hyperebene H des Z-Vektorraumes V punktweise fest. Weil der Rang von H gleich 3 ist, gibt es ein $k \in Z$ mit $h^\alpha = hk$ für alle $h \in H$. (Dies wieder im Vorgriff auf III.1.2.) Wegen $R \subseteq H$ folgt $k = 1$. Dies impliziert wiederum $H = L = R$. Nun hat V aber den Rang 2 über R und den Rang 4 über Z. Das bedeutet, dass R den Rang 2 über Z hat. Damit erhalten wir das widersprüchliche Ergebnis $2 = 3$. Also ist V kein Quaternionenschiefkörper über Z. Daher ist V nach 10.6 ein kommutativer Körper. Dies besagt, dass R, da V im Laufe des Beweises nicht geändert wurde, wie wir bemerkten, im Zentralisator des ursprünglich gewählten Elementes a liegt. Da dieses Element ein beliebiges Element aus $K - R$ war und da R kommutativ ist, liegt R im Zentrum von K entgegen unserer Annahme. Damit ist der Satz in allen seinen Teilen bewiesen.

III.

Gruppen von Kollineationen

Mit jeder Struktur geht ihre Automorphismengruppe einher und das Studium der Automorphismengruppe lässt Rückschlüsse auf die Ausgangsstruktur zu. Dies haben wir in dem uns hier interessierenden Falle der projektiven Geometrien im letzten Kapitel bereits gesehen, wo uns das eingehende Studium der Gruppen $\mathrm{E}(H)$ und $\Delta(P,H)$ zu den Struktursätzen der projektiven Geometrie führte. In diesem Kapitel nun werden wir die volle Kollineationsgruppe einer projektiven Geometrie und gewisse ihrer Untergruppen etwas systematischer studieren.

1. Erste Übersicht

Es sei V ein Vektorraum über dem Körper K. Mit $\Gamma\mathrm{L}(V,K)$ bezeichnen wir die Gruppe aller Automorphismen des K-Vektorraumes V, dh., die Gruppe aller bijektiven semilinearen Abbildungen von V auf sich. Mit $\mathrm{G^*L}(V,K)$ bezeichnen wir die Gruppe aller bijektiven linearen Abbildungen von V auf sich, mit $\mathrm{GL}(V,K)$ die von allen Homothetien und Transvektionen erzeugte Gruppe und mit $\mathrm{SL}(V,K)$ die von allen Transvektionen erzeugte Gruppe. Weil Homothetien und Transvektionen lineare Abbildungen sind, gilt

$$\mathrm{SL}(V,K) \subseteq \mathrm{GL}(V,K) \subseteq \mathrm{G^*L}(V,K) \subseteq \Gamma\mathrm{L}(V,K).$$

Da Transvektionen, Homothetien und lineare Abbildungen unter inneren Automorphismen von $\Gamma\mathrm{L}(V,K)$ wieder in solche übergehen, folgt, dass die Gruppen $\mathrm{SL}(V,K)$ und $\mathrm{GL}(V,K)$ Normalteiler von $\Gamma\mathrm{L}(V,K)$ sind.

1.1. Satz. *Es sei V ein Vektorraum über dem Körper K. Ist der Rang von V mindestens 2 und enthält K mindestens drei Elemente, so wird $\mathrm{GL}(V,K)$ bereits von den Homothetien von V erzeugt.*

Beweis. Es sei τ eine von 1 verschiedene Transvektion von V. Dann gibt es eine lineare Abbildung φ von V in K und einen Vektor $a \in \mathrm{Kern}(\varphi)$ mit $x^\tau = x + a\varphi(x)$ für alle $x \in V$. Weil $\tau \neq 1$ ist, ist $a \neq 0$ und $\mathrm{Kern}(\varphi) \neq V$. Es folgt, dass φ surjektiv ist. Weil K mehr als zwei Elemente enthält, gibt es daher einen Vektor $p \in V$ mit $\varphi(p) \neq 0,\ 1$. Setze $k := -\varphi(p) + 1$. Dann ist $k \neq 0$, so dass k^{-1} existiert. Ferner setzen wir $q := p + a$. Weil p wegen $\varphi(p) \neq 0$ nicht in $H := \mathrm{Kern}(\varphi)$ liegt, liegt q nicht in H, und weil $a \neq 0$ ist, folgt, dass p und q linear unabhängig sind. Somit sind pK und qK zwei verschiedene Komplemente von H. Wir definieren nun zwei Homothetien δ und η vermöge

$(px+h)^\delta := pkx+h$ bzw. $(qx+h)^\eta := qk^{-1}x+h$ für alle $x \in K$ und alle $h \in H$. Dann ist

$$\begin{aligned}(px+h)^{\delta\eta} &= (pkx+h)^\eta = p^\eta kx + h \\ &= (q-a)^\eta kx + h = (qk^{-1}-a)kx + h \\ &= qx - akx + h = px + h + a(1-k)x \\ &= px + h + a\varphi(p)x = px + h + a\varphi(px+h) \\ &= (px+h)^\tau.\end{aligned}$$

Also ist $\delta\eta = \tau$. Damit ist gezeigt, dass alle Transvektionen in der von allen Homothetien erzeugten Gruppe liegen.

Mit $\mathrm{PSL}(V,K)$, $\mathrm{PGL}(V,K)$, $\mathrm{PG^*L}(V,K)$ und $\mathrm{P\Gamma L}(V,K)$ bezeichnen wir die von den Gruppen $\mathrm{SL}(V,K)$, $\mathrm{GL}(V,K)$, $\mathrm{PG^*L}(V,K)$ bzw. $\Gamma\mathrm{L}(V,K)$ in $L_K(V)$ induzierten Kollineationsgruppen. Diese Gruppen heißen der Reihe nach die *kleine projektive Gruppe*, *projektive Gruppe* und *große projektive Gruppe* von $L_K(V)$. Nach II.7.1 ist $\mathrm{P\Gamma L}(V,K)$ die volle Kollineationsgruppe von $L_K(V)$, falls $\mathrm{Rg}_K(V) \geq 3$ ist. Die Gruppe $\mathrm{PGL}(V,K)$ ist dann die von allen Streckungen und Elationen erzeugte Gruppe und wird nach 1.1 bereits von allen Streckungen erzeugt, wenn K mindestens drei Elemente enthält. Die Gruppe $\mathrm{PSL}(V,K)$ ist die Untergruppe von $\mathrm{P\Gamma L}(V,K)$, die von allen Elationen erzeugt wird.

Sind keine Verwechslungen zu befürchten, so lassen wir im Folgenden den zweiten Parameter K bei diesen Gruppen weg.

Wir fragen nun nach dem Kern $M(V)$ des Homomorphismus von $\Gamma\mathrm{L}(V)$ auf $\mathrm{P\Gamma L}(V)$. Ist $\mathrm{Rg}_K(V) = 1$, so ist natürlich $M(V) = \Gamma\mathrm{L}(V)$. Andernfalls gilt:

1.2. Satz. *Es sei V ein Vektorraum über dem Körper K mit $\mathrm{Rg}_K(V) \geq 2$. Dann ist*

$$M(V) = \big\{\mu(k) \mid k \in K^*\big\},$$

wobei $\mu(k)$ die durch $x^{\mu(k)} := xk$ definierte Abbildung ist. Der Zentralisator $C_{\Gamma\mathrm{L}(V)}(M(V))$ von $M(V)$ in $\Gamma\mathrm{L}(V)$ ist gleich $\mathrm{G^*L}(V)$. Ferner gilt

$$M(V) \cap \mathrm{G^*L}(V) = \big\{\mu(k) \mid k \in Z(K^*)\big\}.$$

Beweis. Jedes $\mu(k)$ ist eine bijektive semilineare Abbildung, die alle Punkte von $L_K(V)$ invariant lässt. Somit gilt $\mu(k) \in M(V)$.

Es sei $\rho \in M(V)$. Dann gibt es zu jedem $v \in V - \{0\}$ genau ein $k_v \in K^*$ mit $v^\rho = vk_v$. Sind u, $v \in V - \{0\}$ und ist $u + v \neq 0$, so gilt

$$(u+v)k_{u+v} = (u+v)^\rho = u^\rho + v^\rho = uk_u + vk_v.$$

Sind u und v linear unabhängig, so ist

$$k_u = k_{u+v} = k_v.$$

Sind u und v linear abhängig, ist $uK = vK$. Wegen $\mathrm{Rg}_K(V) \geq 2$ gibt es ein $w \in V - uK$. Dann sind w und u wie auch w und v linear unabhängig. Nach dem bereits Bewiesenen ist daher

$$k_u = k_w = k_v.$$

Hieraus folgt $\rho = \mu(k_u)$, so dass die erste Aussage des Satzes bewiesen ist.

Es sei $\gamma \in C_{\Gamma\mathrm{L}(V)}(M(V))$. Ferner sei α der begleitende Automorphismus von γ. Ist dann $k \in K^*$, so folgt

$$v^\gamma k = v^{\gamma\mu(k)} = v^{\mu(k)\gamma} = (vk)^\gamma = v^\gamma k^\alpha.$$

Also ist $\alpha = 1$ und daher $\gamma \in \mathrm{G^*L}(V)$. Ist umgekehrt $\gamma \in \mathrm{G^*L}(V)$, so ist

$$v^{\gamma\mu(k)} = v^\gamma k = (vk)^\gamma = v^{\mu(k)\gamma},$$

so dass $\gamma \in C_{\Gamma\mathrm{L}(V)}(M(V))$ ist.

Es sei $\mu(k) \in M(V) \cap \mathrm{G^*L}(V)$. Dann ist

$$vlk = (vl)^{\mu(k)} = v^{\mu(k)}l = vkl$$

für alle $v \in V$ und alle $l \in K$. Es folgt $lk = kl$ und damit $k \in Z(K^*)$. Ist umgekehrt $k \in Z(K^*)$, so ist $\mu(k)$ linear, wie man unmittelbar sieht. Damit ist der Satz in allen seinen Teilen bewiesen.

Ist K ein Körper, so bilden die inneren Automorphismen von K eine Gruppe $\mathrm{Inn}(K)$, die sogar ein Normalteiler der Gruppe $\mathrm{Aut}(K)$ ist. Die Faktorgruppe $\mathrm{Aut}(K)/\mathrm{Inn}(K)$ heißt *äußere Automorphismengruppe* von K.

Wir nennen eine Kollineation eines projektiven Raumes *projektiv*, falls sie in der großen projektiven Gruppe enthalten ist.

1.3. Satz. *Ist V ein Vektorraum über dem Körper K mit $\mathrm{Rg}_K(V) \geq 2$, so ist*

$$\mathrm{P\Gamma L}(V)/\mathrm{PG^*L}(V)$$

zur äußeren Automorphismengruppe von K isomorph. Insbesondere gilt: ist $\gamma \in \Gamma\mathrm{L}(V)$, so ist die von γ in $L_K(V)$ induzierte Kollineation genau dann projektiv, wenn der begleitende Automorphismus von γ ein innerer Automorphismus von K ist.

Beweis. Es sei $\gamma \in \Gamma\mathrm{L}(V)$ und α sei der begleitende Automorphismus von γ. Wir nehmen an, dass γ eine projektive Kollineation induziere. Es gibt dann nach 1.2 ein $\delta \in \mathrm{G^*L}(V)$ und ein $k \in K^*$ mit $\gamma\delta^{-1} = \mu(k)$. Weil δ nach 1.2 mit $\mu(k)$ vertauschbar ist, ist $\gamma = \delta\mu(k)$. Ist nun $l \in K$, so folgt

$$v^\delta lk = (vl)^{\delta\mu(k)} = (vl)^\gamma = v^\gamma l^\alpha = v^\delta k l^\alpha.$$

Also ist $l^\alpha = k^{-1}lk$, so dass $\alpha \in \mathrm{Inn}(K)$ gilt.

Es sei umgekehrt $\alpha \in \mathrm{Inn}(K)$. Es gibt dann ein $k \in K^*$ mit $l^\alpha = k^{-1}lk$ für alle $l \in K$. Setze $\delta := \gamma\mu(k^{-1})$. Dann induziert δ die gleiche Kollineation wie γ. Wegen

$$(vl)^\delta = (vl)^\gamma k^{-1} = v^\gamma k^{-1}lkk^{-1} = v^\delta l$$

ist δ linear und γ somit projektiv.

Das bislang Bewiesene zeigt, dass $\mathrm{G^*L}(V)M(V)$ die Menge aller Elemente aus $\Gamma\mathrm{L}(V)$ ist, deren Begleitautomorphismen innere Automorphismen von K

sind. Ist nun β die Abbildung von $\Gamma\mathrm{L}(V)$ in $\mathrm{Aut}(K)$, die jedem Element seinen begleitenden Automorphismus zuordnet, so ist β ein Homomorphismus, der sogar surjektiv ist, wie man unschwer nachprüft. Definiert man nun $\varphi(\gamma)$ für $\gamma \in \Gamma\mathrm{L}(V)$ durch $\varphi(\gamma) := \beta(\gamma)\mathrm{Inn}(K)$, so ist φ ein Epimorphismus von $\Gamma\mathrm{L}(V)$ auf die äußere Automorphismengruppe von K und es gilt, wie wir gesehen haben,

$$\mathrm{Kern}(\varphi) = \mathrm{G}^*\mathrm{L}(V)M(V).$$

Wegen

$$\begin{aligned}\Gamma\mathrm{L}(V)/\mathrm{G}^*\mathrm{L}(V)M(V) &\cong \big(\Gamma\mathrm{L}(V)/M(V)\big)/\big(\mathrm{G}^*\mathrm{L}(V)M(V)/M(V)\big)\\ &= \mathrm{P}\Gamma\mathrm{L}(V)/\mathrm{PG}^*\mathrm{L}(V)\end{aligned}$$

folgt schließlich die noch offene Behauptung des Satzes.

1.4. Satz. *Es sei V ein Vektorraum über K. Sind P und Q Punkte von $L_K(V)$ und ist T ein Teilraum, der weder P noch Q enthält, so gibt es eine Hyperebene $H \in L_K(V)$ mit $T \geq H$ und $P, Q \not\leq H$.*

Beweis. Nach I.1.8 gibt es Hyperebenen H_1 und H_2 mit $T \leq H_i$ und $P + H_1 = V = Q + H_2$. Ist $Q \not\leq H_1$, so ist H_1 eine Hyperebene der gesuchten Art. Ist $P \not\leq H_2$, so ist H_2 eine solche. Wir dürfen also annehmen, dass $P \leq H_2$ und $Q \leq H_1$ ist. Ist dann R ein von P und Q verschiedener Punkt auf $P + Q$, so setzen wir $H := R+(H_1 \cap H_2)$. Wäre H keine Hyperebene, so folgte $R \leq H_1 \cap H_2$ und weiter

$$P \leq P + Q = R + Q \leq H_1.$$

Dieser Widerspruch zeigt, dass H doch eine Hyperebene ist. Mittels des Modulargesetzes folgt

$$\begin{aligned}P + H &= P + R + (H_1 \cap H_2)\\ &= P + Q + (H_1 \cap H_2)\\ &= P + (H_1 \cap (Q + H_2))\\ &= P + H_1 = V.\end{aligned}$$

Ebenso folgt, dass auch $Q + H = V$ ist.

1.5. Satz. *Es sei V ein Vektorraum über dem Körper K und U sei ein Unterraum endlichen Ranges von V. Setze $n := \mathrm{Rg}_K(U)$. Ist $\gamma \in \mathrm{G}^*\mathrm{L}(V)$, so gibt es $\sigma_1, \ldots, \sigma_n \in \mathrm{GL}(V)$ mit den Eigenschaften:*
(1) Jedes σ_i lässt eine Hyperebene vektorweise fest.
(2) $\gamma\sigma_1 \ldots \sigma_n$ lässt U vektorweise fest.

Beweis. Wir machen Induktion nach n. Ist $n = 0$, so ist nichts zu beweisen. Es sei also $n \geq 1$. Ferner sei $U = uK \oplus W$ mit einem $u \neq 0$. Dann ist $\mathrm{Rg}_K(W) = n - 1$, so dass es nach Induktionsannahme $\sigma, \ldots, \sigma_{n-1} \in \mathrm{GL}(V)$ gibt, so dass (1) und (2) gelten, wenn man nur n durch $n - 1$ und U durch W ersetzt. Setze $\rho := \gamma\sigma_1 \ldots \sigma_{n-1}$. Dann gilt u, $u^\rho \in W$. Nach 1.4 gibt es eine Hyperebene H mit $W \subseteq H$, die weder u noch u^ρ enthält. Es gibt daher eine lineare Abbildung σ_n, die H vektorweise festlässt und die u^ρ auf u abbildet. Es

folgt, dass $\rho\sigma_n$ den Teilraum W vektorweise festlässt und dass u ebenfalls von dieser Abbildung festgelassen wird. Weil $\rho\sigma_n$ linear ist und $U = uK \oplus W$ gilt, bleibt jeder Vektor aus U bei $\rho\sigma_n$ fest. Damit ist der Satz bewiesen.

1.6. Satz. *Es sei V ein Vektorraum über dem Körper K. Ist $\sigma \in \mathrm{G^*L}(V)$, so gilt genau dann $\sigma \in \mathrm{GL}(V)$, wenn es einen Unterraum endlichen Ko-Ranges gibt, der von σ vektorweise festgelassen wird.*

Beweis. Ist $\sigma \in \mathrm{GL}(V)$, so ist σ Produkt von endlich vielen Transvektionen und Homothetien. Der Schnitt der Achsen dieser Elationen und Homothetien ist dann ein Unterraum endlichen Ko-Ranges, der von σ vektorweise festgelassen wird.

Es sei $W := \{v \mid v \in V, v^\sigma = v\}$ und W habe endlichen Ko-Rang. Setze $n := \mathrm{KoRg}_K(W)$. Ist $n = 0$, so ist nichts zu beweisen. Es sei also $n > 0$ und $b_1, \ldots, b_n$ seien n linear unabhängige Vektoren, die nicht in W liegen. Dann ist auch $b_n^\sigma \notin W$. Nach 1.4 gibt es also eine Hyperebene H die zwar W, nicht aber b_n und b_n^σ enthält. Es gibt daher ein $\tau \in \mathrm{GL}(V)$, welches H vektorweise festlässt und b_n^σ auf b_n abbildet. Dann lässt aber $\sigma\tau$ den Unterraum $b_nK + W$ vektorweise fest, so dass Induktion zum Ziele führt.

1.7. Satz. *Ist V ein Vektorraum über dem Körper K so sind die folgenden Aussagen äquivalent:*
a) $\mathrm{Rg}_K(V)$ *ist endlich.*
b) *Es ist* $\mathrm{GL}(V) = \mathrm{G^*L}(V)$.
c) *Es ist* $\mathrm{PGL}(V) = \mathrm{PG^*L}(V)$.

Beweis. a) impliziert b): Dies folgt mit 1.6.

b) impliziert c): Banal.

c) impliziert a): Wir zeigen, dass die Verneinung von a) die Verneinung von c) nach sich zieht. Ist der Rang von V nicht endlich, so gibt es eine abzählbare Teilmenge $\{b_i \mid i \in \omega\}$ von linear unabhängigen Vektoren in V. Es sei

$$U := \sum_{i:=0}^{\infty} b_i K$$

und W sei ein Komplement von U in V. Wir definieren $\sigma \in \mathrm{G^*L}(V)$ durch $b_i^\sigma := b_i + b_{i+1}$ und $w^\sigma := w$ für alle $i \in \omega$ und alle $w \in W$. Es sei vK ein Fixpunkt von σ. Es gibt dann ein $n \in \omega$, sowie $k_0, \ldots, k_n \in K$ und ein $w \in W$ mit

$$v = \sum_{i:=0}^{n} b_i k_i + w.$$

Weil vK ein Fixpunkt ist, gibt es ein $a \in K^*$ mit

$$\sum_{i:=0}^{n} b_i k_i a + wa = va = v^\sigma = \sum_{i:=0}^{n} b_i^\sigma k_i + w = \sum_{i:=0}^{n} (b_i + b_{i+1}) k_i + w.$$

Hieraus folgt $0 = k_n$ und $k_i a = k_i + k_{i-1}$ für $i := 0, \ldots, n$. Dies hat zur Folge, dass alle k_i gleich Null sind. Somit gilt $vK \subseteq W$. Wäre nun die von σ induzierte

Kollineation ein Element von $\mathrm{PGL}(V)$, so wäre diese Kollineation ein Produkt von endlich vielen Elationen und Streckungen. Der Schnitt ihrer Achsen wäre ein Teilraum endlichen Ko-Ranges in V. Dieser Teilraum läge nach unserer Vorbemerkung aber in W, so dass W endlichen Ko-Rang hätte, was nicht der Fall ist. Damit ist alles bewiesen.

Als Nächstes wollen wir die pappösschen Räume mittels ihrer Kollineationsgruppen charakterisieren. Dazu beweisen wir zunächst den folgenden Satz.

1.8. Satz. *Es sei V ein Vektorraum über dem Körper K und U sei ein Teilraum von V mit $2 \leq \mathrm{Rg}_K(U) < \infty$. Setze $n := \mathrm{Rg}_K(U)$. Ist dann $P_0, \ldots, P_n$ ein Rahmen von U, so gibt es Vektoren $v_0, \ldots, v_n$ mit $P_i = v_iK$ für $i := 0, \ldots, n$ und $v_0 = \sum_{i:=1}^n v_i$.*

Beweis. Es sei $P_i = u_iK$. Weil $P_1, \ldots, P_n$ eine Basis von U ist, gibt es $k_i \in K$ mit $u_0 = \sum_{i:=1}^n u_ik_i$. Weil je n der $n+1$ Punkte eines Rahmens von U eine Basis von U bilden, folgt, dass die k_i allesamt ungleich Null sind. Setzt man daher $v_0 := u_0$ und $v_i := u_ik_i$ für $i := 1, \ldots, n$, so tun's diese v_i.

1.9. Satz. *Es sei V ein Vektorraum über dem Körper K. Ferner sei n eine natürliche Zahl größer als 1. Sind dann U und W zwei Unterräume des Ranges n von V, ist $P_0, \ldots, P_n$ ein Rahmen von U und $Q_0, \ldots, Q_n$ ein solcher von W, so gibt es ein $\sigma \in \mathrm{PGL}(V)$ mit $P_i^\sigma = Q_i$ für $i := 1, \ldots, n$. Ist der Rang von V endlich, so ist $\mathrm{PGL}(V)$ also transitiv auf der Menge der Rahmen von V.*

Beweis. Nach I.7.2 haben U und W ein gemeinsames Komplement C in V. Nach 1.8 gibt es ferner $u_0, \ldots, u_n$ und $w_0, \ldots, w_n$ mit $P_i = u_iK$ und $Q_i = w_iK$ für $i := 0, \ldots, n$ sowie $u_0 = \sum_{i:=1}^n u_i$ und $w_0 = \sum_{i:=1}^n w_i$. Definiert man nun ρ durch $c^\rho := c$ für alle $c \in C$ und $u_i^\rho := v_i$ für $i := 1, \ldots, n$, so ist ρ nach 1.6 ein Element in $\mathrm{GL}(V)$. Da offenbar $u_0^\rho = w_0$ ist, leistet die von ρ induzierte Kollineation σ das Verlangte.

Es sei V ein Vektorraum des Ranges 2 über dem Körper K. Motiviert durch den Satz II.6.3 nennen wir $L(V)$ pappossch, wenn K kommutativ ist.

1.10. Satz. *Es sei V ein Vektorraum über dem Körper K und es gelte $\mathrm{Rg}_K(V) \geq 2$. Dann sind äquivalent:*

a) *$L_K(V)$ ist pappossch.*

b) *Ist U ein Teilraum des endlichen Ranges $n \geq 2$ von V, ist $P_0, \ldots, P_n$ ein Rahmen von U, ist $\sigma \in \mathrm{PG^*L}(V)$ und gilt $P_i^\sigma = P_i$ für $i := 0, \ldots, n$, so induziert σ auf $U/0$ die Identität.*

c) *Es gibt einen Teilraum U des endlichen Ranges $n \geq 2$ von V und einen Rahmen $P_0, \ldots, P_n$ von U, so dass jedes $\sigma \in \mathrm{PGL}(V)$, für das $P_i^\sigma = P_i$ für $i := 0, \ldots, n$ gilt, auf $U/0$ die Identität induziert.*

Beweis. a) impliziert b): Nach II.6.3 ist K kommutativ. Davon werden wir gleich Gebrauch machen.

Es sei nun $P_i = u_iK$ und es gelte $u_0 = \sum_{i:=1}^n u_i$. Es sei $\sigma \in \mathrm{G^*L}(V)$ und es gelte $P_i^\sigma = P_i$ für alle i. Es gibt dann $k_i \in K^*$ mit $u_i^\sigma = u_ik_i$ für alle i. Es folgt

$$\sum_{i:=1}^n u_ik_i = \left(\sum_{i:=1}^n u_i\right)^\sigma = u_0^\sigma = u_0k_0 = \sum_{i:=1}^n u_ik_0.$$

Wegen der linearen Unabhängigkeit von $u_1, \ldots, u_n$ folgt $k_0 = k_1 = \ldots = k_n$. Ist nun $v \in U$, so gilt $v = \sum_{i:=1}^{n} u_i a_i$ mit gewissen $a_i \in K$. Hieraus folgt zusammen mit der Kommutativität von K, dass

$$v^\sigma = \sum_{i:=1}^{n} u_i k_0 a_i = \left(\sum_{i:=}^{n} u_i a_i\right) k_0 = v k_0$$

ist. Somit gilt b).

b) impliziert c): Weil der Rang von V mindestens 2 ist, ist c) natürlich eine Folge von b).

c) impliziert a): Es gibt wieder $u_i \in U$ mit $P_i = u_i K$ und $u_0 = \sum_{i:=1}^{n} u_i$. Es sei $k \in K^*$. Dann ist $u_1 k, \ldots, u_n k$ eine Basis von U. Unter Zuhilfenahme eines Komplementes von U folgt die Existenz eines $\sigma \in \mathrm{GL}(V)$ mit $u_i^\sigma = u_i k$ für $i := 1, \ldots, n$. Es folgt, dass auch $u_0^\sigma = u_0 k$ ist. Also ist $P_i^\sigma = P_i$ für alle i, so dass σ nach Voraussetzung auf der Menge der Punkte von $L_K(V)$ die Identität induziert. Mit Satz 1.2 folgt, dass $v^\sigma = vk$ gilt für alle $v \in U$ und dass darüber hinaus k ein Element von $Z(K)$ ist, da σ ja in $\mathrm{GL}(V)$ liegt. Also ist $K^* \subseteq Z(K)$, so dass a) eine Folge von c) ist.

1.11. Korollar. *Es sei V ein Vektorraum über dem Körper K mit $2 \leq \mathrm{Rg}_K(V) < \infty$. Genau dann ist $L_K(V)$ pappossch, wenn* $\mathrm{PGL}(V)$ *auf der Menge der Rahmen von $L_K(V)$ scharf transitiv operiert.*

Beweis. Dies folgt unmittelbar aus 1.9 und 1.10.

Ist V ein Vektorraum endlichen Ranges über einem kommutativen Körper und ist $\gamma \in \mathrm{GL}(V)$, so bezeichnen wir mit $\det(\gamma)$ die Determinante von γ.

1.12. Satz. *Ist V ein Vektorraum über dem kommutativen Körper K mit $1 \leq \mathrm{Rg}_K(V) < \infty$, so gilt:*
a) *Die Abbildung* det *ist ein Homomorphismus von* $\mathrm{GL}(V)$ *auf* K^*.
b) $\mathrm{SL}(V)$ *ist der Kern von* det.

Beweis. a) Nach 1.7 ist $\mathrm{GL}(V) = \mathrm{G}^*\mathrm{L}(V)$, so dass a) dem Leser aus dem Anfängerunterricht bekannt sein sollte.

b) Es sei $V = P \oplus H$ mit einem Punkt P und einer Hyperebene H. Dann ist $\mathrm{SL}(V)\Sigma(P, H) \subseteq \mathrm{GL}(V)$, wobei $\Sigma(P, H)$ wieder die Gruppe aller Homothetien mit dem Zentrum P und der Achse H bezeichne. Da die Gruppe $\mathrm{SL}(V)$ auf der Menge der nicht inzidenten Punkt-Hyperebenenpaare von $L(V)$ transitiv operiert, enthält $\mathrm{SL}(V)\Sigma(P, H)$ alle Homothetien. Daher ist $\mathrm{SL}(V)\Sigma(P, H) = \mathrm{GL}(V)$.

Es sei τ eine Transvektion. Es gibt dann eine lineare Abbildung φ von V auf K und ein $a \in \mathrm{Kern}(\varphi)$ mit $x^\tau = x + a\varphi(x)$ für alle $x \in V$. Ist $b_1, \ldots, b_n$ eine Basis von V mit $b_2, \ldots, b_n \in H$, so wird τ bezüglich dieser Basis durch eine Dreiecksmatrix mit lauter Einsen auf der Hauptdiagonalen dargestellt. Daher ist $\det(\tau) = 1$, so dass $\mathrm{SL}(V) \subseteq \mathrm{Kern}(\det)$ gilt. Ist nun $\kappa \in \mathrm{Kern}(\det)$, so gibt es ein $\sigma \in \mathrm{SL}(V)$ und ein $k \in K^*$ mit $\kappa = \sigma\delta(k)$. Es folgt $\det(\kappa) = \det(\delta(k))$. Wählt man nun eine Basis $b_1, \ldots, b_n$ mit $b_1 \in P$ und $b_2, \ldots, b_n \in H$, so sieht man, dass $\delta(k)$ durch eine Diagonalmatrix dargestellt wird, wo an der

ersten Stelle der Diagonalen k^{-1} steht und alle übrigen Diagonalelemente gleich 1 sind. Also ist

$$1 = \det(\kappa) = k^{-1},$$

so dass $k = 1$ und damit $\kappa \in \mathrm{SL}(V)$ ist.

Wir sind nun in der Lage, die Ordnungen der Gruppen $\Gamma\mathrm{L}(V)$ etc. auszurechnen, falls V ein endlicher Vektorraum ist. Ist V ein Vektorraum des Ranges n über $\mathrm{GF}(q)$, so schreiben wir statt $\Gamma\mathrm{L}(V)$, usw., $\Gamma\mathrm{L}(n,q)$, usw.

1.13. Satz. *Sind n und r natürliche Zahlen, ist p eine Primzahl und ist $q := p^r$, so gilt:*

a) $|\Gamma\mathrm{L}(n,q)| = rq^{\frac{1}{2}n(n-1)} \prod_{i:=1}^{n}(q^i - 1)$.

b) $|\mathrm{GL}(n,q)| = q^{\frac{1}{2}n(n-1)} \prod_{i:=1}^{n}(q^i - 1)$.

c) $|SL(n,q)| = q^{\frac{1}{2}n(n-1)} \prod_{i:=2}^{n}(q^i - 1)$.

d) $|\mathrm{P}\Gamma\mathrm{L}(n,q)| = rq^{\frac{1}{2}n(n-1)} \prod_{i:=2}^{n}(q^i - 1)$.

e) $|\mathrm{PGL}(n,q)| = q^{\frac{1}{2}n(n-1)} \prod_{i:=2}^{n}(q^i - 1)$.

f) $|\mathrm{PSL}(n,q)| = \mathrm{ggT}(n,q-1)^{-1} q^{\frac{1}{2}n(n-1)} \prod_{i:=2}^{n}(q^i - 1)$.

Beweis. Da alle endlichen Körper kommutativ sind, ist die Gruppe $\mathrm{PGL}(n,q)$ auf der Menge der Rahmen des zu Grunde liegenden projektiven Raumes nach 1.11 scharf transitiv. Mit I.7.9 folgt daher

$$\bigl|\mathrm{PGL}(n,q)\bigr| = q^{\frac{1}{2}n(n-1)} \prod_{i:=2}^{n}(q^i - 1).$$

Aus 1.7 und 1.3 folgt, dass $\mathrm{P}\Gamma\mathrm{L}(n,q)/\mathrm{PGL}(n,q)$ zu $\mathrm{Aut}(\mathrm{GF}(q))$ isomorph ist. Also ist

$$|\mathrm{P}\Gamma\mathrm{L}(n,q)| = \bigl|\mathrm{Aut}(GF(q))\bigr|\,\bigl|\mathrm{PGL}(n,q)\bigr| = r\bigl|\mathrm{PGL}(n,q)\bigr|.$$

Aus 1.2 folgt, dass der Kern M des Homomorphismus der Gruppe $\mathrm{GL}(n,q)$ auf die Gruppe $\mathrm{PGL}(n,q)$ die Ordnung $q-1$ hat. Daher ist

$$\bigl|\mathrm{GL}(n,q)\bigr| = (q-1)\bigl|\mathrm{PGL}(n,q)\bigr|.$$

Wegen $\Gamma\mathrm{L}(n,q)/GL(n,q) \cong (\Gamma\mathrm{L}(n,q)/M)/(\mathrm{GL}(n,q)/M)$ ist

$$\bigl|\Gamma\mathrm{L}(n,q)\bigr| = r\bigl|\mathrm{GL}(n,q)\bigr|.$$

Schließlich folgt aus 1.12

$$\bigl|\mathrm{GL}(n,q)\bigr| = (q-1)\bigl|\mathrm{SL}(n,q)\bigr|.$$

Ist σ eine Abbildung aus dem Kern des Homomorphismus von $\mathrm{SL}(n,q)$ auf $\mathrm{PSL}(n,q)$, so ist $v^\sigma = vk$ für alle $v \in V$ und einem passenden $k \in K^*$. Es folgt $1 = \det(\sigma) = k^n$. Die Anzahl der Lösungen dieser Gleichungen ist aber gleich $\mathrm{ggT}(n,q-1)$, da die multiplikative Gruppe zyklisch ist. Daher ist

$$\bigl|\mathrm{PSL}(n,q)\bigr| = \mathrm{ggT}(n,q-1)^{-1}\bigl|\mathrm{SL}(n,q)\bigr|.$$

Damit ist alles bewiesen.

2. Die Einfachheit der kleinen projektiven Gruppe

In diesem Abschnitt wollen wir zeigen, dass die Gruppen $\mathrm{PSL}(V)$ bis auf zwei Ausnahmen einfache Gruppen sind, dh., dass sie nur die beiden unvermeidbaren Normalteiler haben, die jede Gruppe hat. Auf dem Wege dorthin und als Folgerungen daraus werden wir noch eine Reihe weiterer interessanter Ergebnisse gewinnen. Zunächst müssen wir aber unser Vokabular erweitern.

Wir haben in Kapitel II häufig den Begriff der Transitivität einer Gruppe benutzt, der Begriff der Bahn ist aber noch nicht gefallen. Hier seine Definition. Es sei G eine Permutationsgruppe auf der Menge M. Definiert man auf M die Relation $\sim$ durch $x \sim y$ genau dann, wenn es ein $\gamma \in G$ gibt mit $x^\gamma = y$, so folgt, dass $\sim$ eine Äquivalenzrelation ist. Die Äquivalenzklassen von $\sim$ heißen *Bahnen* von G auf M. Ist M selbst eine Bahn, so ist das gleichbedeutend mit der Transitivität von G auf M.

Es sei G transitiv auf M. Gibt es eine Teilmenge T von M, die wenigstens zwei Elemente enthält, jedoch von M verschieden ist, und gilt, dass für alle $\gamma \in G$, für die $T \cap T^\gamma \neq \emptyset$ ist, $T = T^\gamma$ ist, so sagen wir, dass G auf M *imprimitiv* operiere und dass T ein *Imprimitivitätsgebiet* von G sei. Gibt es kein solches T, so operiert G auf M *primitiv*.

Es sei N ein Normalteiler von G und T sei eine Bahn von N. Ist $\gamma \in G$, so ist auch T^γ eine Bahn von N. Aus $T \cap T^\gamma \neq \emptyset$ folgt daher, dass $T = T^\gamma$ ist. Ist $N \neq \{1\}$, so folgt aus der Transitivität von G auf M, dass alle Bahnen von N gleichmächtig sind und wenigstens zwei Elemente enthalten. Ist $T \neq M$, so ist T also ein Imprimitivitätsgebiet von G. Ist G primitiv, so ist jeder von $\{1\}$ verschiedene Normalteiler von G transitiv auf M.

Ist G eine Gruppe, so bezeichnen wir mit G' die *Kommutatorgruppe* von G, das ist die von allen *Kommutatoren* $a^{-1}b^{-1}ab$ mit $a, b \in G$ erzeugte Untergruppe von G. Es folgt, dass G' ein Normalteiler von G ist und dass G/G' abelsch ist. Es folgt ferner, dass G' in allen Normalteilern N von G enthalten ist, für die G/N abelsch ist. G' ist also der kleinste unter diesen Normalteilern.

Die *absteigende Kommutatorreihe* der Gruppe G ist rekursiv definiert durch $G^{(0)} := G$ und $G^{(i+1)} := (G^{(i)})'$. Die Gruppe G heißt *auflösbar*, wenn es ein n gibt mit $G^{(n)} = \{1\}$. Sie heißt *perfekt*, wenn $G = G'$ ist.

Diese Begriffe werden nun zur Formulierung eines von Iwasawa stammenden Satzes benutzt (Iwasawa 1962).

2.1. Satz. *Ist G eine Permutationsgruppe auf der Menge M, operiert G auf M primitiv, ist G perfekt und enthält der Stabilisator eines Elementes aus M in G einen auflösbaren Normalteiler, der zusammen mit seinen Konjugierten die Gruppe G erzeugt, so ist G einfach.*

Beweis. Es sei N ein nicht trivialer Normalteiler von G. Da G primitiv ist, operiert N nach obiger Bemerkung auf M transitiv. Es sei $m \in M$ und B sei der nach Voraussetzung existierende Normalteiler von G_m, der zusammen mit seinen Konjugierten die Gruppe G erzeugt. Es sei $\gamma \in G$. Wegen der Transitivität von N auf M gibt es ein $\nu \in N$ mit $m^{\gamma\nu} = m$. Weil B in G_m

normal ist, folgt $(\gamma\nu)^{-1}B(\gamma\nu) = B$. Folglich ist

$$\gamma^{-1}B\gamma = \nu B\nu^{-1}.$$

Somit enthält die Gruppe NB alle zu B in G konjugierten Untergruppen. Dies besagt, dass $G = NB$ ist.

Es ist also $G = NB^{(0)}$. Es sei $i \leq 0$ und es gelte $G = NB^{(i)}$. Dann ist

$$G/N = (NB^{(i)})/N \cong B^{(i)}/(B^{(i)} \cap N).$$

Wegen $G' = G$ gibt es kein von $\{1\}$ verschiedenes epimorphes Bild von G/N, welches abelsch ist. Daher ist $B^{(i)} = B^{(i+1)}(B^{(i)} \cap N)$. Hieraus folgt weiter

$$G = NB^{(i)} = NB^{(i+1)}(B^{(i)} \cap N) = NB^{(i+1)}.$$

Weil B auflösbar ist, gibt es ein n mit $B^{(n)} = \{1\}$. Daher ist $G = N$, womit die Einfachheit von G nachgewiesen ist.

2.2. Satz. *Es sei V ein Vektorraum über dem Körper K. Dann gilt:*

a) *Ist* $\mathrm{Rg}_K(V) = 2$*, so ist* $\mathrm{PSL}(V)$ *auf der Menge der Punkte von* $L_K(V)$ *zweifach transitiv.*

b) *Ist* $\mathrm{Rg}_K(V) \geq 3$*, so ist* $\mathrm{PSL}(V)$ *auf der Menge der Tripel* (P, Q, H) *transitiv, wobei P und Q zwei verschiedene Punkte und H eine Hyperebene von $L_K(V)$ ist, die weder P noch Q enthält. Insbesondere ist* $\mathrm{PSL}(V)$ *auf der Menge der Punkte von $L_K(V)$ zweifach transitiv.*

Beweis. a) Ist H eine Hyperebene von V, was im vorliegenden Falle gleichbedeutend damit ist, dass H ein Punkt ist, so permutiert die Gruppe $\mathrm{T}(H)$ aller Transvektionen mit der Achse H die von H verschiedenen Punkte transitiv. Da der Punkt H kein Fixpunkt von $\mathrm{PSL}(V)$ ist, ist diese Gruppe also auf der Menge der Punkte von $L_K(V)$ zweifach transitiv.

b) Es seien (P, Q, H) und (P', Q', H') zwei Tripel der verlangten Art. Nach II.3.2 operiert $\mathrm{PSL}(V)$ auf der Menge der nicht inzidenten Punkt-Hyperebenenpaare transitiv. Wir dürfen daher annehmen, dass $P = P'$ und $H = H'$ ist. Wir dürfen ferner annehmen, dass $Q \not\leq Q'$ ist. Dann ist $Q + Q'$ eine Gerade von $L_K(V)$.

1. Fall: Es ist $P \not\leq Q + Q'$. Wir setzen $R := (Q + Q') \cap H$. Dann ist R ein Punkt, da $Q + Q'$ eine Gerade ist, die nicht in H liegt. Nach 1.4 gibt es eine Hyperebene H^* mit $P + R \leq H^*$ und $Q,\ Q' \not\leq H^*$. Es gibt also eine Elation $\tau \in \mathrm{E}(R, H^*)$ mit $Q^\tau = Q'$. Nun ist $P \leq H^*$ und $R \leq H$. Daher ist $P^\tau = P$ und $H^\tau = H$. Damit ist in diesem Falle alles bewiesen.

2. Fall: Es ist $P \leq Q + Q'$. Wegen $\mathrm{Rg}_K(V) \geq 3$, gibt es einen Punkt S mit $S \not\leq Q + Q'$ und $S \not\leq H$. Dann erfüllen die beiden Tripelpaare (P, Q, H), (P, S, H) und (P, S, H), (P, Q', H) die Voraussetzungen des Falles 1, so dass Fall 2 auf diesen zurückgeführt ist.

Dass $\mathrm{PSL}(V)$ auf der Menge der Punkte von $L_K(V)$ zweifach transitiv operiert, folgt schließlich daraus, dass zwei Punkte von $L_K(V)$ nach 1.4 stets ein gemeinsames Komplement besitzen.

2.3. Satz. *Ist V ein Vektorraum über dem Körper K, so gilt:*

a) *Ist* $\mathrm{Rg}_K(V) = 2$*, so sind alle von* 1 *verschiedenen Transvektionen in* $\mathrm{GL}(V)$ *konjugiert.*

b) *Ist* $\mathrm{Rg}_K(V) \geq 3$*, so sind alle von* 1 *verschiedenen Transvektionen in* $\mathrm{SL}(V)$ *konjugiert.*

Beweis. a) Es seien σ und τ zwei von 1 verschiedene Transvektionen. Dann gibt es zwei linear unabhängige Vektoren a und b, so dass

$$(ar + bs)^\sigma = a(r + s) + bs,$$

und zwei linear unabhängige Vektoren c und d, so dass

$$(cr + ds)^\tau = c(r + s) + bs$$

ist für alle r, $s \in K$. Es gibt ferner eine $\gamma \in \mathrm{GL}(V)$ mit $a^\gamma = c$ und $b^\gamma = d$. Hiermit folgt

$$(cr + ds)^{\gamma^{-1}\sigma\gamma} = (ar + bs)^{\sigma\gamma} = \bigl(a(r + s) + bs\bigr)^\gamma = c(r + s) + ds = (cr + ds)^\gamma.$$

Also ist $\gamma^{-1}\sigma\gamma = \tau$, womit a) bewiesen ist.

b) Es seien σ und τ von 1 verschiedene Transvektionen. Wie üblich stellen wir sie dar durch $x^\sigma = x + a\varphi(x)$ und $x^\tau = x + b\psi(x)$. Dann sind $H := \mathrm{Kern}(\varphi)$ und $H' := \mathrm{Kern}(\psi)$ zwei Hyperebenen. Es seien P und Q Punkte mit $P \not\leq H$ und $Q \not\leq H'$. Dann ist auch $P^\sigma \not\leq H$ und $Q^\tau \not\leq H'$. Es gibt ein $p \in P$ mit $\varphi(p) = 1$ und ein $q \in Q$ mit $\psi(q) = 1$. Es gilt $p^\sigma = p + a$ und $q^\tau = q + b$.

Nach 2.2 gibt es ein $\gamma \in \mathrm{SL}(V)$ mit $P^\gamma = Q$, $P^{\sigma\gamma} = Q^\tau$ und $H^\gamma = H'$. Es folgt $p^\gamma = qk$, $p^{\sigma\gamma} = q^\tau m$ und wegen $aK = (P + P^\sigma) \cap H$ und $bK = (Q + Q^\tau) \cap H'$ auch $a^\gamma = bn$ mit k, m, $n \in K^*$. Somit ist

$$qk + bn = p^\gamma + a^\gamma = (p + a)^\gamma = p^{\sigma\gamma} = q^\tau m = (q + b)m = qm + bm.$$

Weil q und b linear unabhängig sind, folgt $k = m = n$. Ist nun $r \in K$ und $h \in H'$, so folgt wegen $h^{\gamma^{-1}} \in H$, dass $h^{\gamma^{-1}\sigma\gamma} = h$ ist. Hiermit folgt weiter

$$\begin{aligned}(qr + h)^{\gamma^{-1}\sigma\gamma} &= q^{\gamma^{-1}\sigma\gamma} r + h = \bigl(q^{\gamma^{-1}} + a\varphi(q^{\gamma^{-1}})\bigr)^\gamma r + h \\ &= qr + h + a^\gamma\varphi(pk^{-1})r = qr + h + bkk^{-1}r \\ &= qr + h + b\psi(qr + h) = (qr + h)^\tau.\end{aligned}$$

Also ist $\gamma^{-1}\sigma\gamma = \tau$, so dass σ und τ, wie behauptet, in $\mathrm{SL}(V)$ konjugiert sind.

2.4. Satz. *Es sei V ein Vektorraum über dem Körper K und es gelte* $V = u_1K \oplus u_2K \oplus W$ *mit von* 0 *verschiedenen Vektoren u_1 und u_2. Ist dann* $a \in K^*$*, so liegt die durch*

$$(u_1r + u_2s + w)^\sigma := u_1ar + u_2a^{-1}s + w$$

definierte Abbildung σ in $\mathrm{SL}(V)$.

Beweis. Für $i := 1, 2$ setzen wir $H_i := u_iK + W$. Dann sind H_1 und H_2 Hyperebenen von $L_K(V)$. Wir definieren Transvektionen τ_1, τ_2, τ_3 und τ_4 durch

$$\begin{aligned}(u_2r + h_1)^{\tau_1} &= u_2r + h_1 - u_1r\\ (u_1r + h_2)^{\tau_2} &= u_1r + h_2 - u_2(1-a)a^{-1}r\\ (u_2r + h_1)^{\tau_3} &= u_2r + h_1 + u_1ar\\ (u_1r + h_2)^{\tau_4} &= u_1r + h_2 + u_2(1-a)a^{-2}r,\end{aligned}$$

wobei die h_i Elemente aus H_i bezeichnen. Eine einfache Rechnung zeigt dann, dass $\sigma = \tau_1\tau_2\tau_3\tau_4$ ist.

2.5. Satz. *Ist V ein Vektorraum über dem Körper K mit* $\mathrm{Rg}_K(V) \geq 2$*, so ist* $\mathrm{SL}(V)$ *perfekt, es sei denn, es ist* $\mathrm{Rg}_K(V) = 2$ *und* $|K| = 2$ *oder* $|K| = 3$.

Beweis. Auf Grund von 2.3 genügt es zu zeigen, dass die $\mathrm{SL}(V)$ unter den gemachten Voraussetzungen eine Transvektion enthält, die der Kommutator zweier Elemente aus $\mathrm{SL}(V)$ ist.

1. Fall: $\mathrm{Rg}_K(V) = 2$. Dann ist $V = uK \oplus vK$. Weil K mindestens 4 Elemente enthält, gibt es ein $a \in K$, welches von 0, 1 und -1 verschieden ist. Nach 2.4 liegt die durch

$$(ur + vs)^\sigma := uar + va^{-1}s$$

definierte Abbildung σ in $\mathrm{SL}(V)$. Wir definieren ferner eine Transvektion τ durch

$$(ur + vs)^\tau := ur + v(s - r).$$

Dann ist, wie man leicht nachrechnet,

$$(ur + vs)^{\sigma^{-1}\tau^{-1}\sigma\tau} = ur + vs + v(a^{-2} - 1)r.$$

Dies zeigt, dass $\sigma^{-1}\tau^{-1}\sigma\tau$ eine Transvektion ist, die von 1 verschieden ist, da ja $a \neq 1, -1$ ist.

2. Fall: Es ist $\mathrm{Rg}_K(V) \geq 3$. Es seien H und H' zwei verschiedene Hyperebenen von $L_K(V)$ und φ seien zwei Linearformen auf V mit $H = \mathrm{Kern}(\varphi)$ und $H' = \mathrm{Kern}(\psi)$. Weil der Rang von V mindestens gleich 3 ist, gibt es ein von Null verschiedenes $b \in H \cap H'$. Es sei ferner $a \in H - H'$. Wir definieren die Transvektionen σ und τ durch $x^\sigma := x + a\varphi(x)$ und $x^\tau := x + b\psi(x)$. Eine einfache Rechnung zeigt dann, dass

$$x^{\sigma^{-1}\tau^{-1}\sigma\tau} = x + b\psi(a)\varphi(x)$$

ist. Nun ist $\psi(a) \neq 0$, da ja $a \notin H' = \mathrm{Kern}(\psi)$ ist. Also ist $\sigma^{-1}\tau^{-1}\sigma\tau$ eine von 1 verschiedene Transvektion, so dass der Satz auch im zweiten Falle etabliert ist.

2.6. Satz. *Ist V ein Vektorraum über dem Körper K mit* $\mathrm{Rg}_K(V) \geq 2$*, so ist* $\mathrm{PSL}(V)$ *einfach, es sei denn, es ist* $\mathrm{Rg}_K(V) = 2$ *und* $|K| = 2$ *oder* $|K| = 3$.

Beweis. Es sei $|K| \geq 4$, falls $\mathrm{Rg}_K(V) = 2$ ist. Nach 2.5 ist $\mathrm{SL}(V)$ dann perfekt, so dass auch $\mathrm{PSL}(V)$ perfekt ist. Ferner gilt, dass $\mathrm{PSL}(V)$ auf der Menge der Punkte von $L_K(V)$ zweifach transitiv operiert, also erst recht primitiv. Ist P ein Punkt, so ist die Gruppe $\mathrm{E}(P)$ aller Elationen mit dem Zentrum P ein abelscher Normalteiler von $\mathrm{PSL}(V)_P$, der zusammen mit seinen Konjugierten die Gruppe $\mathrm{PSL}(V)$ erzeugt. Da abelsche Gruppe natürlich auflösbar sind, folgt aus dem Satz 2.1 von Iwasawa, dass $\mathrm{PSL}(V)$ einfach ist.

Nach 1.13 ist $|\mathrm{PSL}(2,2)| = 2 \cdot 3$ und $|\mathrm{PSL}(2,3)| = 3 \cdot 4$, so dass diese Gruppen auflösbar sind. Im Falle der $\mathrm{PSL}(2,2)$ gibt es nämlich $3 \cdot 1$ Elemente der Ordnung 2, die von Transvektionen induziert werden. Zusammen mit den 3 Elementen einer 3-Sylowgruppe erhält man alle 6 Elemente der $\mathrm{PSL}(2,2)$, so dass die 3-Sylowgruppe von $\mathrm{PSL}(2,2)$ ein Normalteiler dieser Gruppe ist. Im Falle der $\mathrm{PSL}(2,3)$ gibt es $4 \cdot 2 = 8$ Elemente der Ordnung 3, die von Transvektionen induziert werden. Zusammen mit den 4 Elementen einer 2-Sylowgruppe erhält man alle 12 Elemente von $\mathrm{PSL}(2,3)$, so dass in diesem Falle die 2-Sylowgruppe normal ist. Somit sind diese beiden Gruppen wirkliche Ausnahmen zu Satz 2.6.

2.7. Satz. *Ist V ein Vektorraum über dem Körper K, ist $\mathrm{Rg}_K(V) \geq 2$ und ist $|K| > 2$, falls $\mathrm{Rg}_K(V) = 2$, so gilt:*

a) *Es ist* $\mathrm{GL}(V)' = \mathrm{SL}(V)$.

b) *Es ist* $\mathrm{PGL}(V)' = \mathrm{PSL}(V)$.

Beweis. Wir beginnen mit einer Vorbemerkung. Es sei G eine Gruppe, S ein Normalteiler und U eine Untergruppe von G. Ferner sei S perfekt und $G = SU$. Da S als Untergruppe von SU' diese Gruppe normalisiert und da S und U' von U normalisiert werden, folgt, dass SU' ein Normalteiler von $SU = G$ ist. Daher ist

$$G/(SU') = \big(SU'U\big)/(SU') \cong U/\big(U \cap SU'\big).$$

Wegen $U' \subseteq U \cap SU'$ ist $U/(U \cap SU')$ und damit $G/(SU')$ abelsch. Also ist

$$G' \subseteq SU' = S'U' \subseteq G'$$

und folglich $G' = SU'$.

Es sei nun $G := \mathrm{GL}(V)$, $S := \mathrm{SL}(V)$ und $U := \sum(P,H)$, wobei P ein Punkt und H eine Hyperebene von V sei mit $V = P \oplus H$. Ist dann $|K| > 3$, falls $\mathrm{Rg}_K(V) = 2$ ist, so folgt mit der Vorbemerkung und Satz 2.5, dass

$$\mathrm{GL}(V)' = \mathrm{SL}(V)\Sigma(P,H)'$$

ist. Wir müssen also zeigen, dass $\Sigma(P,H)' \subseteq \mathrm{SL}(V)$ ist. Dazu seien $a, b \in K^*$. Setze $c := b^{-1}a^{-1}ba$. Wir zeigen, dass $\delta(c) \in \mathrm{SL}(V)$ ist.

Es sei $P = uK$ und $H = vK \oplus W$ mit $v \neq 0$. Wir definieren Abbildungen σ_1, σ_2 und σ_3 durch

$$\begin{aligned}
(ur + vs + w)^{\sigma_1} &:= ubr + vb^{-1}s + w,\\
(ur + vs + w)^{\sigma_2} &:= uar + va^{-1}s + w,\\
(ur + vs + w)^{\sigma_3} &:= ua^{-1}b^{-1}r + vbas + w
\end{aligned}$$

für alle r, $s \in K$ und alle $w \in W$. Nach 2.4 ist dann $\sigma_i \in \mathrm{SL}(V)$ für alle i. Dann ist aber auch $\sigma_1\sigma_2\sigma_3 \in \mathrm{SL}(V)$. Eine einfache Rechnung zeigt, dass

$$(ur + vs + w)^{\sigma_1\sigma_2\sigma_3} = uc^{-1}r + vs + w = (ur + vs + w)\delta(c)$$

ist. Folglich ist $\delta(c) = \sigma_1\sigma_2\sigma_3$, so dass in der Tat

$$\Sigma(p, H)' \subseteq \mathrm{SL}(V)$$

ist. Daher ist $\mathrm{GL}(V)' = \mathrm{SL}(V)$.

Es sei nun $|K| = 3$ und $V = uK \oplus vK$. Dann ist K kommutativ. Die Gruppe $\sigma(uK, vK)$ ist zur multiplikativen Gruppe von K isomorph, also abelsch. Wegen $\mathrm{GL}(V) = \mathrm{SL}(V)\Sigma(uK, vK)$ ist daher $G' \subseteq \mathrm{SL}(V)$. Es sei τ eine nicht triviale Transvektion mit dem Zentrum vK. Dann ist $(ur + vs)^\tau = ur + vs + var$ mit $a \in K^*$. Ferner ist die durch $(ur + vs)^\sigma := ur - vs$ definierte Abbildung σ ein Element aus $\mathrm{GL}(V)$. Dann ist aber

$$(ur + vs)^{\sigma^{-1}\tau^{-1}\sigma\tau} = ur + vs + 2var = ur + vs - var = (ur + vs)^{\tau^{-1}},$$

so dass jede Transvektion ein Kommutator in $\mathrm{GL}(V)$ ist. Also ist $\mathrm{SL}(V) \subseteq \mathrm{GL}(V)'$, so dass a) bewiesen ist.

b) ist eine einfache Folgerung aus a).

Wir haben gerade gesehen, dass $\Sigma(P, H)' \subseteq \mathrm{SL}(V) \cap \Sigma(P, H)$ ist. Wissbegierig wie wir sind, stellen wir die Frage, ob vielleicht

$$\Sigma(P, H)' = SL(V) \cap \Sigma(P, H)$$

ist. Im Falle eines kommutativen Körpers und endlicher Dimension von V ist das ja so, wie wir beim Beweise von 1.13 gesehen haben. Diese Gleichheit gilt in der Tat immer, wie wir im nächsten Abschnitt sehen werden.

2.8. Satz. *Es sei V ein Vektorraum über dem Körper K mit $\mathrm{Rg}_K(V) \geq 2$. Ist V nicht der Vektorraum vom Range 2 über $\mathrm{GF}(2)$ oder $\mathrm{GF}(3)$ und ist N eine von $\{1\}$ verschiedene Untergruppe von $\mathrm{PG^*L}(V)$, die von $\mathrm{PSL}(V)$ normalisiert wird, so ist $\mathrm{PSL}(V) \subseteq N$.*

Beweis. Wir beginnen wieder mit einer Vorbemerkung, die dem, der sich mit Permutationsgruppen auskennt, geläufig ist. Es seien M und N zwei Normalteiler der Gruppe G mit $M \cap N = \{1\}$. Ist $m \in M$ und $n \in N$, so ist $n^{-1}m^{-1}n \in M$ und daher $n^{-1}m^{-1}nm \in M$. Andererseits ist $m^{-1}nm \in N$ und daher auch $n^{-1}m^{-1}nm \in N$. Also ist

$$n^{-1}m^{-1}nm \in M \cap N = \{1\}.$$

Dies zeigt, dass M und N sich gegenseitig zentralisieren. Ist überdies G eine auf der Menge Ω primitive Permutationsgruppe, so sind M und N beide transitiv, falls sie beide von $\{1\}$ verschieden sind. Es sei $\alpha \in \Omega$, $m \in M$ und es gelte $\alpha^m = \alpha$. Ist dann $n \in N$, so ist

$$\alpha^{nm} = \alpha^{mn} = \alpha^n,$$

so dass auch α^n ein Fixelement von m ist. Wegen der Transitivität von N auf Ω folgt daher $m = 1$. Folglich ist M auf Ω scharf transitiv. Ebenso folgt natürlich, dass auch N auf Ω scharf transitiv operiert.

Zurück zu unserem Satz. Weil N von $\mathrm{PSL}(V)$ normalisiert wird, ist $G := \mathrm{PSL}(V)N$ eine Untergruppe von $\mathrm{PG^*L}(V)$ und $\mathrm{PSL}(V)$ und N sind Normalteiler dieser Gruppe. Weil $\mathrm{PSL}(V)$ auf der Menge der Punkte von $L_K(V)$ nach 2.2 zweifach transitiv operiert, operiert sie auf dieser Menge erst recht primitiv. Wäre nun $\mathrm{PSL}(V) \not\subseteq N$, so folgte $\mathrm{PSL}(V) \cap N = \{1\}$, da $\mathrm{PSL}(V)$ unter den gemachten Voraussetzungen ja einfach ist. Nach unserer Vorbemerkung folgte dann aber, dass $\mathrm{PSL}(V)$ auf der Menge der Punkte von $L_K(V)$ scharf transitiv operierte. Dieser Widerspruch zeigt, dass doch $\mathrm{PSL}(V) \subseteq N$ gilt.

2.9. Korollar. *Es sei V ein Vektorraum über dem Körper K, dessen Rang mindestens 2 sei. Ferner sei $|K| > 3$, falls $\mathrm{Rg}_K(V) = 2$ ist. Ist N eine Untergruppe von $\mathrm{G^*L}(V)$, die von $\mathrm{SL}(V)$ normalisiert wird, so ist N entweder im Zentrum von $\mathrm{G^*L}(V)$ enthalten oder aber N enthält $\mathrm{SL}(V)$.*

Beweis. Ist $k \in K^*$, so sei $\mu(k)$, wie schon zuvor, die durch $v^{\mu(k)} := vk$ definierte Abbildung von V auf sich und $M(V)$ bezeichne die Gruppe aller dieser $\mu(k)$. Ist Z das Zentrum von $\mathrm{G^*L}(NV)$, so gilt nach 1.2, dass $M(V) \cap \mathrm{G^*L}(V) \subseteq Z$ ist. Wäre $M(V) \cap \mathrm{G^*L}(V) \neq Z$, so induzierte Z einen von $\{1\}$ verschiedenen abelschen Normalteiler in $\mathrm{PG^*L}(V)$, der nach 2.8 die nicht abelsche Gruppe $\mathrm{PSL}(V)$ enthielte. Also ist doch $M(V) \cap \mathrm{G^*L}(V) = Z$.

Die fragliche Gruppe N sei nicht in Z enthalten. Wegen $Z = M(V) \cap \mathrm{G^*L}(V)$ induziert N dann eine nicht triviale Untergruppe N' in $\mathrm{PG^*L}(V)$, die von $\mathrm{PSL}(V)$ normalisiert wird. Nach 2.8 ist daher $\mathrm{PSL}(V) \subseteq N'$. Hieraus folgt, dass $\mathrm{SL}(V) \subseteq NZ$ ist. Nun ist $(NZ)/N \cong Z/(N \cap Z)$, so dass $(NZ)/N$ abelsch ist. Daher ist $(NZ)' \subseteq N$ und weiter

$$\mathrm{SL}(V) = \mathrm{SL}(V)' \subseteq (NZ)' \subseteq N.$$

Damit ist das Korollar bewiesen.

Die Sätze 2.7 und 2.9 geben eine vollständige Übersicht über alle Normalteiler von $\mathrm{GL}(V)$. Ist der Rang von V nicht endlich, so bleiben noch die Normalteiler von $\mathrm{G^*L}(V)$ zu bestimmen. Der interessierte Leser findet eine vollständige Übersicht über die Normalstruktur von $\mathrm{G^*L}(V)$ in Rosenberg 1958.

3. Determinanten

In diesem Abschnitt soll nun das Versprechen eingelöst werden, den Beweis dafür zu liefern, dass $\Sigma(P,H)' = \mathrm{SL}(V) \cap \Sigma(P,H)$ ist. Dazu benötigen wir die von Dieudonné eingeführte Determinantenfunktion für Endomorphismen von Vektorräumen über nicht notwendig kommutativen Körpern. Die hier angegebene koordinatenfreie Konstruktion der Determinantenfunktion stammt von U. Dempwolff. Es ist zu beachten, dass man die Determinantenfunktion ohne Umschweife für jeden, also auch nicht endlich erzeugten Vektorraum V auf $\mathrm{GL}(V)$ definieren kann. (Dempwolff 1993, Dieudonné 1943, Lüneburg 1993, S. 193ff.)

Wir beginnen damit, eine gemeinsame Beschreibung der Dilatationen und Transvektionen zu geben. Da wir im Folgenden ständig Dilatationen und Transvektionen unter dem gleichen Blickwinkel betrachten, geben wir der Menge aus Dilatationen und Transvektionen eines Vektorraumes den Namen Σ. Man beachte, dass auch $1_V \in \Sigma$ ist.

3.1. Satz. *Es sei V ein Vektorraum über dem Körper K und Σ sei die Menge der Dilatationen und Transvektionen von V.*
a) *Ist $\sigma \in \Sigma$, so gibt es ein $a \in V$ und ein $f \in V^*$ mit $f(a) \neq 1$ und*

$$v^\sigma = v - af(v)$$

für alle $v \in V$. Ist σ nicht die Identität, so ist $a \neq 0$ und auch $f \neq 0$.
b) *Ist $v^\sigma = v - af(v)$ und $v^\tau = v - a'f'(v)$, und ist σ, $\tau \neq 1_V$, so ist genau dann $\sigma = \tau$, wenn es ein $k \in K^*$ gibt mit $a' = ak$ und $f' = k^{-1}f$.*

Beweis. a) Es sei σ eine Transvektion und H sei ihre Achse. Es gibt dann *per definitionem* ein $f \in V^*$ mit $\mathrm{Kern}(f) = H$ sowie ein $a \in H$, so dass $v^\tau = v + af(v)$ ist. Indem man a durch $-a$ ersetzt, erhält man für τ die Darstellung

$$v^\tau = v - af(v).$$

Überdies ist $f(a) = 0$ und daher $f(a) \neq 1$.

Es sei σ eine Dilatation mit der Achse H und dem Zentrum P. Ferner sei $0 \neq a \in P$. Ist dann $v \in V$, so gibt es ein $k \in K$ und ein $h \in H$ mit $v = ak + h$. Es gibt ferner ein $b \in K^*$ mit $(ak + h)^\sigma = abk + h$. Definiere $f \in V^*$ durch

$$f(ak + h) := (1 - b)k.$$

Dann ist

$$(ak + h)^\delta = abk + h = ak + h - a(1 - b)k = ak + h - af(ak + h),$$

m. a. W., es ist

$$v^\delta = v - af(v)$$

für alle $v \in V$. Weil δ injektiv ist, ist $f(a) \neq 1$. Die restliche Aussage von a) versteht sich von selbst.

b) Es sei $\sigma = \tau$. Dann ist $v - af(v) = v - a'f'(v)$ und damit $af(v) = a'f'(v)$ für alle $v \in V$. Weil σ nicht die Identität ist, ist $f' \neq 0$. Es gibt also ein v mit $f'(v) = 1$. Setze $k := f(v)$. Dann ist $k \in K^*$ und es gilt $a' = ak$. Es folgt $af(v) = akf'(v)$. Wiederum weil σ nicht die Identität ist, ist $a \neq 0$. Es folgt $f(v) = kf'(v)$ für alle $v \in V$. Die Umkehrung ist banal. Also gilt auch b).

Es sei $\sigma \in \Sigma$. Dann gibt es einen Vektor $a \in V$ und ein $f \in V^*$ mit $x^\sigma = x - af(x)$ für alle $x \in V$. Ist auch $x^\sigma = x - a'f'(x)$, so gibt es nach 3.1 b) ein $k \in K^*$ mit $a' = ak$ und $f' = k^{-1}f$. Da $f(a) \neq 1$ ist folgt,

$$\begin{aligned} 1 - f'(a') &= 1 - k^{-1}f(ak) = k^{-1}\bigl(1 - f(a)\bigr)k \\ &= \bigl(1 - f(a)\bigr)\bigl(1 - f(a)\bigr)^{-1}k^{-1}\bigl(1 - f(a)\bigr)k. \end{aligned}$$

Setzt man nun

$$\det(\sigma) := \bigl(1 - f(a)\bigr)(K^*)',$$

so ist det also eine wohldefinierte Abbildung von Σ in die Kommutatorfaktorgruppe $K^*/(K^*)'$.

Ist $\sigma \in \Sigma$ und ist $\tau \in \mathrm{GL}(V)$, ist ferner $v^\sigma = v - af(v)$, so folgt

$$v^{\tau^{-1}\sigma\tau} = v - a^\tau f(v\tau^{-1}).$$

Hieraus folgt weiter

$$\det(\tau^{-1}\sigma\tau) = \bigl(1 - f(a^{\tau\tau^{-1}})\bigr)(K^*)' = \det(\sigma),$$

so dass det unter Konjugation invariant bleibt.

Ist K ein Körper, so setzen wir im Folgenden

$$K_A := K^*/(K^*)'.$$

Den kanonischen Epimorphismus von K^* auf K_A bezeichnen wir mit π.

3.2. Satz. *Es sei V ein Vektorraum über dem Körper K und Σ sei die Menge der Transvektionen und Dilatationen von V. Sind σ, $\tau \in \Sigma$ und haben σ und τ das gleiche Zentrum oder die gleiche Achse, so ist auch $\sigma\tau \in \Sigma$ und es gilt* $\det(\sigma\tau) = \det(\sigma)\det(\tau)$.

Beweis. Wir betrachten zunächst den Fall, dass σ und τ das gleiche Zentrum haben. Es gibt dann ein $a \in V$ und f, $g \in V^*$ mit $v^\sigma = v - af(v)$ und $v^\tau = v - ag(v)$. Es folgt

$$\begin{aligned} v^{\sigma\tau} &= \bigl(v - af(v)\bigr)^\tau = v^\tau - a^\tau f(v) \\ &= v - ag(v) - \bigl(a - ag(a)\bigr)f(v) \\ &= v - a\bigl(g(v) + f(v) - g(a)f(v)\bigr). \end{aligned}$$

Daher ist $\sigma\tau \in \Sigma$ und es gilt

$$\begin{aligned} \det(\sigma\tau) &= \pi\bigl(1 - g(a) - f(a) + g(a)f(a)\bigr) \\ &= \pi\bigl(1 - g(a)\bigr)\pi\bigl(1 - f(a)\bigr) \\ &= \det(\sigma)\det(\pi), \end{aligned}$$

da die Multiplikation in K_A ja kommutativ ist.

Es bleibt der Fall zu betrachten, dass σ und π die gleiche Achse haben. Dann gibt es a, $b \in V$ und ein $f \in V^*$ mit $v^\sigma = v - af(v)$ und $v^\tau = v - bf(v)$. Es folgt

$$\begin{aligned} v^{\sigma\tau} &= \bigl(v - af(v)\bigr)^\tau \\ &= v^\tau - a^\tau f(v) \\ &= v - bf(v) - \bigl(a - bf(a)\bigr)f(v) \\ &= v - \bigl(b + a - bf(a)\bigr)f(v). \end{aligned}$$

Also ist $\sigma\tau \in \Sigma$ und

$$\begin{aligned}\det(\sigma\tau) &= \pi\bigl(1 - f(b + a - bf(a)\bigr)\\ &= \pi\bigl(1 - f(b) - f(a) + f(b)f(a)\bigr)\\ &= \pi\bigl(1 - f(b)\bigr)\pi\bigl(1 - f(a)\bigr)\\ &= \det(\sigma)\det(\tau).\end{aligned}$$

Damit ist der Satz bewiesen.

Bei diesem Beweis haben wir zweimal von der Kommutativität von K_A Gebrauch gemacht. Das ist der Sache nicht inhärent, liegt vielmehr daran, dass wir die Abbildungen auf die gleiche Seite wie die Skalare schreiben, nämlich als Exponenten rechts von den Vektoren.

3.3. Satz. *Es sei V ein K-Vektorraum und Σ sei die Menge der Transvektionen und Dilatationen von V. Sind σ_1, $\sigma_2 \in \Sigma$ und haben σ_1 und σ_2 verschiedene Zentren P_1 und P_2 und verschiedene Achsen und ist P ein Punkt auf der Geraden $P_1 + P_2$, so gibt es τ_1, $\tau_2 \in \Sigma$ mit den folgenden Eigenschaften:*
a) *τ_2 hat Zentrum P.*
b) *Es ist $\sigma_1\sigma_2 = \tau_1\tau_2$.*
c) *Es ist* $\det(\sigma_1)\det(\sigma_2) = \det(\tau_1)\det(\tau_2)$.

Beweis. Ist $P = P_2$, so tun es $\tau_1 := \sigma_1$ und $\tau_2 := \sigma_2$. Ist $P = P_1$, so tun es $\tau_1 := \sigma_1\sigma_2\sigma_1^{-1}$ und $\tau_2 := \sigma_1$.

Es sei $P \neq P_1$, P_2. Ist $0 \neq a_1 \in P_1$ und $0 \neq a_2 \in P_2$, so gibt es f_1, $f_2 \in V^*$ mit

$$v^{\sigma_i} = v - a_i f_i(v)$$

für $i := 1$, 2 und alle $v \in V$. Setze $H_i := \mathrm{Kern}(f_i)$. Nach 3.2 hängt H_i nur von σ_i, nicht aber von der Wahl von $a_i \in P_i$ ab. Davon werden wir im Folgenden Gebrauch machen, indem wir die a_i der Situation entsprechend wählen.

Setze $D := H_1 \cap H_2$ sowie $G := P_1 + P_2$. Nach Voraussetzung ist dann

$$\mathrm{Rg}_K(G) = 2 = \mathrm{KoRg}_K(D).$$

Es sei $P_1 \leq H_2$. Hier wählen wir die a_i so, dass $P = (a_1 + a_2)K$ gilt. Hiermit definieren wir τ_1 und τ_2 durch

$$v^{\tau_1} := v - a_1(f_1 - f_2)(v)$$

bzw.

$$v^{\tau_2} := v - (a_1 + a_2)f_2(v).$$

Dann ist $a_1^{\tau_2} = a_1 = a_1^{\sigma_2}$ und daher

$$\begin{aligned}v^{\tau_1\tau_2} &= \bigl(v - a_1(f_1(v) - f_2(v)r)\bigr)^{\tau_2}\\ &= v^{\tau_2} - a_1 f_1(v) + a_1 f_2(v)\\ &= v - (a_1 + a_2)f_2(v) - a_1 f_1(v) + a_1 f_2(v)\\ &= v - a_1 f_1(v) - a_2 f_2(v)\\ &= v^{\sigma_1\sigma_2}.\end{aligned}$$

Ferner ist

$$\det(\tau_1) = \pi\big(1 - f_1(a_1) + f_2(a_1)\big) = \pi\big(1 - f_1(a_1)\big) = \det(\sigma_1)$$

und

$$\det(\tau_2) = \pi\big(1 - f_2(a_1 + a_2)\big) = \pi\big(1 - f_2(a_2)\big) = \det(\sigma_2)$$

Es sei $P_2 \leq H_1$. Wegen $\sigma_1\sigma_2 = \sigma_1\sigma_2\sigma_1^{-1}\sigma_1$ erledigt sich dies mit dem gerade behandelten Fall.

Wir dürfen daher im Folgenden annehmen, dass $P_1 \not\leq H_2$ und $P_2 \not\leq H_1$ gilt. Dann ist P_1, $P_2 \not\leq D$ und folglich

$$\mathrm{Rg}_K(G \cap D) \leq 1.$$

Es sei C ein Komplement von $G \cap D$ in D. Weil σ_1 und σ_2 auf C die Identität induzieren, dürfen wir annehmen, dass $C = \{0\}$ ist. Dann ist also $D \leq G$ und $\mathrm{Rg}_K(D) \leq 1$.

1. Fall: Es ist $\mathrm{Rg}_K(D) = 1$. Dann ist $\mathrm{Rg}_K(V) = 3$. Wegen P_1, $P_2 \neq D$ können wir die a_i so wählen, dass

$$D = (a_1 + a_2)K$$

ist. Setze $b_1 := a_1 + a_2$ und $b_2 := a_1$. Dann ist b_1, b_2 eine Basis von G. Wegen $P \neq P_1 = b_2K$ gibt es also ein $x \in K$ mit

$$P = (b_1 + xb_2)K.$$

Es sei $b_3 \in H_2 - D$. Dann ist $b_3 \notin G$, da $g \cap H_2 = D$ ist. Folglich ist $\{b_1, b_2, b_3\}$ eine Basis von V. Ferner gilt, man beachte, dass $b_1 \in D = H_1 \cap H_2$ ist,

$$b_1^{\sigma_1} = b_1$$

und, mit implizit definierten u, $v \in K$,

$$\begin{aligned} b_2^{\sigma_1} &= a_1 - a_1 f_1(a_1) \\ &= a_2\big(1 + f_1(a_2)\big) - (a_1 + a_2) f_1(a_2) \\ &= b_2\big(1 - f_1(b_2)\big) - b_1 f_1(b_2) \\ &= b_1 u + b_2 v, \end{aligned}$$

sowie

$$b_3^{\sigma_1} = b_3.$$

Entsprechend erhalten wir

$$b_1^{\sigma_2} = b_1$$

und, mit wiederum implizit definierten y, $z \in K$,

$$b_2^{\sigma_2} = a_2 - a_2 f_2(a_2) = b_2\big(1 - f_2(b_2)\big) = b_2 y$$

sowie

$$b_3^{\sigma_2} = b_3 - a_2 f_2(b_3) = b_3 - b_2 f_2(b_3) = b_2 z + b_3.$$

Es folgt

$$\begin{aligned} b_1^{\sigma_1\sigma_2} &= b_1 \\ b_2^{\sigma_1\sigma_2} &= b_1 u + b_2 yv \\ b_3^{\sigma_1\sigma_2} &= b_2 z + b_3. \end{aligned}$$

Wir setzen $s := 1$, falls $x = 0$, dh., falls $P = b_1 K$ ist, und $s := x^{-1}$, falls $x \neq 0$ ist. Wir definieren nun Abbildungen τ_1 und τ_2 durch

$$\begin{aligned} b_1^{\tau_1} &:= b_1 \\ b_2^{\tau_1} &:= b_1\big(u + s(1-yv)\big) + b_2 \\ b_3^{\tau_1} &:= -b_1 sz + b_3 \end{aligned} \qquad \text{und} \qquad \begin{aligned} b_1^{\tau_2} &:= b_1 \\ b_2^{\tau_2} &:= b_1 s(yv-1) + b_2 yv \\ b_3^{\tau_2} &:= b_1 sz + b_2 z + b_3. \end{aligned}$$

Einfache Rechnungen zeigen, dass $b_i^{\sigma_1\sigma_2} = b_i^{\tau_1\tau_2}$ ist für alle i. Somit ist $\sigma_1\sigma_2 = \tau_1\tau_2$.

Ist $v = b_1 x_1 + b_2 x_2 + b_3 x_3$, so folgt

$$v^{\tau_1} = v - b_1\big(szx_3 - (u + s(1-yv))x_2\big)$$

und

$$v^{\tau_2} = v - (b_1 s + b_2)\big((1-yv)x_2 - zx_3)\big),$$

so dass $\tau_i \in \Sigma$ gilt. Ferner ist $\det(\tau_1) = \pi(1)$ und $\det(\tau_i) = \pi(yv)$. Es bleibt die Aussage über das Zentrum von τ_2 zu beweisen.

Ist $x \neq 0$, so ist $s = x^{-1}$ und daher

$$(b_1 s + b_2)K = (b_1 + b_2 x)K = P.$$

Ist $x = 0$, so ist $s = 0$ und P ist das Zentrum von τ_1. Dann folgt aber mit $\tau_1\tau_2 = \tau_1\tau_2\tau_1^{-1}\tau_1$ und Ersetzen von τ_1 und τ_2 durch $\tau_1\tau_2\tau^{-1}$ und τ_1 die Behauptung.

2. Fall: Es ist $D = \{0\}$. In diesem Falle wählen wir die a_i so, dass $P = (a_1 - a_2)K$ ist. Wir definieren u, v, x, $y \in K$ durch

$$\begin{aligned} a_1^{\sigma_1} &= a_1\big(1 - f_1(a_1)\big) = a_1 u \\ a_2^{\sigma_1} &= a_2 - a_1 f_1(a_2) = a_1 v + a_2 \end{aligned}$$

und

$$\begin{aligned} a_1^{\sigma_2} &= a_1 - a_2 f_2(a_1) = a_1 + a_2 x \\ a_2^{\sigma_2} &= a_2\big(1 - f_2(a_2)\big) = a_2 y. \end{aligned}$$

Es folgt

$$\begin{aligned} a_1^{\sigma_1\sigma_2} &= a_1 u + a_2 xu \\ a_2^{\sigma_1\sigma_2} &= a_1 v + a_2(xv + y). \end{aligned}$$

Es ist $\det(\sigma_1) = \pi(u)$ und $\det(\sigma_2) = \pi(y)$. Wir haben nun zwei Fälle zu unterscheiden.

2.1. Fall: Es ist $u = v$. In diesem Falle definieren wir τ_1 und τ_2 durch

$$\begin{aligned} a_1^{\tau_1} &:= a_1(1 - xu) + a_2xu \\ a_2^{\tau_1} &:= a_1(1 - xu - y) + a_2(xu + y) \end{aligned}$$

und

$$\begin{aligned} a_1^{\tau_2} &:= a_1u \\ a_2^{\tau_2} &:= a_1u + a_2. \end{aligned}$$

Eine einfache Rechnung zeigt, dass

$$a_1^{\tau_1\tau_2} = a_1u + a_2xu = a_1^{\sigma_1\sigma_2}$$

und

$$a_2^{\tau_1\tau_2} = a_1u + a_2(xu + y)$$

ist. Wegen $u = v$ ist also auch

$$a_2^{\tau_1\tau_2} = a_2^{\sigma_1\sigma_2},$$

so dass $\sigma_1\sigma_2 = \tau_1\tau_2$ ist. Ist $v = a_1k_1 + a_2k_2$, so folgt

$$v_1^{\tau} = v - (a_1 - a_2)\big(xuk_1 + (y + xu - 1)k_2\big)$$

und

$$\det(\tau_1) = \pi\big(1 - xu - (y + xu - 1)(-1)\big) = \pi(y)$$

sowie

$$v^{\tau_2} = v - a_1\big((1 - u)k_1 - uk_2\big)$$

und

$$\det(\tau_2) = \pi(1 - 1 + u) = \pi(u).$$

Weil die Multiplikation in K_A kommutativ ist, ist also

$$\det(\sigma_1)\det(\sigma_2) = \det(\tau_1)\det(\tau_2).$$

Ferner ist P das Zentrum von τ_1, woraus mit der schon mehrfach angewandten Identität $\tau_1\tau_2 = (\tau_1\tau_2)\tau_1^{-1}\tau_1$ die Behauptung in diesem Falle folgt.

2.2. Fall: Es ist $u \neq v$. Hier definieren wir τ_1 und τ_2 durch

$$\begin{aligned} a_1^{\tau_1} &:= a_1u + a_2(1 - u) \\ a_2^{\tau_1} &:= a_1v + a_2(1 - v) \end{aligned}$$

und

$$\begin{aligned} a_1^{\tau_2} &:= a_1 + a_2\big(x + y(u - v)^{-1}(u - 1)\big) \\ a_2^{\tau_2} &:= a_2y(u - v)^{-1}u. \end{aligned}$$

Dann ist wieder $\sigma_1\sigma_2 = \tau_1\tau_2$. Ferner gilt, falls $v = a_1k_1 + a_2k_2$ ist,

$$v^{\tau_1} = v - (a_1 - a_2)\big((1 - u)k_1 - vk_2\big)$$

und daher

$$\det(\tau_1) = \pi\big(1 - (1-u) - v(-1)\big) = \pi(u-v)$$

sowie

$$v^{\tau_2} = v - a_2\big((x + y(u-v)^{-1}(1-u)k_1 - (y(u-v)^{-1}u + 1)k_2)\big)$$

und folglich

$$\det(\tau_2) = \pi\big(1 + (y(u-v)^{-1}u + 1)(-1)\big) = \pi\big(y(u-v)^{-1}u\big).$$

Der Punkt P ist wieder Zentrum von τ_1. Aus all diesem folgt auch in diesem letzten Fall die Behauptung des Satzes, wobei wieder zu beachten ist, dass K_A eine abelsche Gruppe ist.

3.4. Satz. *Es sei V ein Vektorraum über dem Körper K und Σ sei die Menge der Dilatationen und Transvektionen von V. Sind $\sigma_1, \ldots, \sigma_n \in \Sigma$ und gilt*

$$\sigma_1 \cdots \sigma_n = 1,$$

so ist

$$\det(\sigma_1) \cdots \det(\sigma_n) = 1.$$

Beweis. Wir machen Induktion nach n. Für $n = 1$ ist der Satz richtig. Es sei $n = 2$. Dann ist also $1 = \sigma_1\sigma_2$. Es folgt, dass σ_1 und σ_2 gleiches Zentrum und gleiche Achse haben. Nach 3.2 ist daher

$$1 = \det(1) = \det(\sigma_1)\det(\sigma_2).$$

Es sei $n \geq 3$ und der Satz gelte für $n-1$. Ferner sei

$$\sigma_1 \cdots \sigma_n = 1.$$

Gibt es ein i, so dass σ_i und σ_{i+1} gleiches Zentrum oder gleiche Achse haben, so ist $\sigma_i\sigma_{i+1} \in \Sigma$ und $\det(\sigma_i\sigma_{i+1}) = \det(\sigma_i)\det(\sigma_{i+1})$. Nun ist

$$\sigma_1 \cdots (\sigma_i\sigma_{i+1}) \cdots \sigma_n = 1.$$

Nach Induktionsannahme ist daher

$$\det(\sigma_1) \cdots \det(\sigma_n) = \det(\sigma_1) \cdots \det(\sigma_i\sigma_{i+1}) \cdots \det(\sigma_n) = 1.$$

Es bleibt der Fall zu betrachten, dass σ_i und σ_{i+1} für $i := 1, \ldots, n-1$ verschiedene Zentren und verschiedene Achsen haben. Es sei P_i das Zentrum von σ_i. Dann ist

$$\sigma_n^{-1} = \sigma_1 \cdots \sigma_{n-1}$$

und P_n ist auch das Zentrum von σ_n^{-1}. Setze

$$H := P_1 + \ldots + P_{n-1}.$$

Weil σ_i auf V/P_i die Identität induziert, induziert σ_i auch auf V/H die Identität. Somit induziert auch σ_n^{-1} auf V/H die Identität, da σ_n^{-1} ja das Produkt von σ_1, …, σ_{n-1} ist. Es folgt

$$P_n = V^{\sigma_n^{-1}-1} \leq H,$$

da P_n ja auch das Zentrum von σ_n^{-1} ist.

Es sei r eine natürliche Zahl. Ferner seien $\tau_1, \ldots, \tau_r \in \Sigma$ und Q_r sei das Zentrum von τ_r. Schließlich gelte

$$\sigma_n^{-1} = \tau_1 \cdots \tau_r \sigma_{r+1} \cdots \sigma_{n-1}$$

und

$$P_n \leq Q_r + P_{r+1} + \ldots + P_{n-1}$$

sowie

$$\det(\sigma_1) \cdots \det(\sigma_{n-1}) = \det(\tau_1) \cdots \det(\tau_r) \det(\sigma_{r+1}) \cdots \det(\sigma_{n-1}).$$

Für $r = 1$ erhält man diese Situation, indem man $\tau_1 = \sigma_1$ und $Q_1 := P_1$ setzt, wie wir gerade gesehen haben. Es sei $1 \leq r < n-1$ und es mögen $\tau_1, \ldots, \tau_r$ mit den verlangten Eigenschaften geben. Ist $Q_r = P_{r+1}$ oder ist die Achse von τ_r gleich der Achse von σ_{r+1}, so schließt man wie zuvor, dass

$$\det(\sigma_1) \cdots \det(\sigma_n) = 1$$

ist. Es sei also $Q_r \neq P_{r+1}$ und auch die Achsen von τ_r und σ_{r+1} seien verschieden.

Es sei $P_i = a_i K$ für $i := 1, \ldots, n$ und $Q_r = b_r K$. Wegen $P_n \leq Q_r + P_{r+1} + \ldots + P_{n-1}$ gibt es $k_r, \ldots, k_{n-1} \in K$ mit

$$a_n = b_r k_r + a_{r+1} k_{r+1} + \ldots + a_{n-1} k_{n-1}.$$

Ist $b_r k_r + a_{r+1} k_{r+1} \neq 0$, so setzen wir

$$Q_{r+1} := (b_r k_r + a_{r+1} k_{r+1}) K.$$

Ist $b_r k_r + a_{r+1} k_{r+1} = 0$, so sei Q_{r+1} ein beliebiger Punkt auf der Geraden $Q_r + P_{r+1}$. In jedem Falle gilt

$$P_n \leq Q_{r+1} + P_{r+2} + \ldots + P_{n-1}.$$

Nach Satz 3.3 gibt es τ_r', $\tau_{r+1} \in \Sigma$ mit

$$\tau_r \sigma_{r+1} = \tau_r' \tau_{r+1},$$

so dass Q_{r+1} das Zentrum von τ_{r+1} ist und überdies

$$\det(\tau_r) \det(\sigma_{r+1}) = \det(\tau_r') \det(\tau_{r+1})$$

gilt. Ersetzt man τ_r durch τ_r', so hat man die Induktion um einen Schritt weitergetrieben oder aber erkannt, dass der Satz auch für n gilt. Wir dürfen daher annehmen, dass es $\tau_1, \ldots, \tau_{n-1} \in \Sigma$ gibt mit

$$\sigma_n = \tau_1 \cdots \tau_{n-1}$$

und

$$\det(\sigma_1) \cdots \det(\sigma_{n-1}) = \det(\tau_1) \cdots \det(\tau_{n-1}),$$

so dass P_n auch Zentrum von τ_{n-1} ist. Setze $\rho := \tau_{n-1}\sigma_n$. Nach Satz 3.2 ist $\rho \in \Sigma$ und es gilt $\det(\rho) = \det(\tau_{n-1})\det(\sigma_n)$. Es folgt

$$1 = \tau_1 \cdots \tau_{n-2}\rho$$

und daher

$$1 = \det(\tau_1) \cdots \det(\tau_{n-2})\rho = \det(\sigma_1) \cdots \det(\sigma_n).$$

Damit ist der Satz bewiesen.

3.5. Satz. *Es sei V ein Vektorraum über dem Körper K und Σ sei die Menge der Dilatationen und Transvektionen von V. Ist $\gamma \in \mathrm{GL}(V)$, so gibt es $\sigma_1, \ldots, \sigma_n \in \Sigma$ mit $\gamma = \sigma_1 \cdots \sigma_n$. Setzt man*

$$\det(\gamma) := \det(\sigma_1) \cdots \det(\sigma_n),$$

so ist det *ein Homomorphismus von $\mathrm{GL}(V)$ auf $K^*/(K^*)'$ und es gilt, falls $\mathrm{Rg}_K(V) \geq 2$ ist,*

$$\mathrm{Kern}(\det) = \mathrm{SL}(V).$$

Beweis. Mit 3.4 folgt, dass det wohldefiniert ist. Dass det dann ein Epimorphismus ist, ist banal. Es bleibt die Aussage über den Kern von det zu beweisen.

Ist τ eine Transvektion, so ist $\det(\tau) = 1$, wie wir wissen. Daher gilt $\mathrm{SL}(V) \subseteq \mathrm{Kern}(\det)$.

Es sei $\alpha \in \mathrm{Kern}(\det)$. Ferner sei $V = P \oplus H$ mit einem Punkt P und einer Hyperebenen H. Dann ist, wie wir wissen, $\mathrm{GL}(V) = \mathrm{SL}(V)\Sigma(P,H)$. Es gibt also ein $\sigma \in \mathrm{SL}(V)$ und ein $k \in K^*$ mit $\alpha = \sigma\delta(k)$. Es folgt

$$\pi(1) = \det(\alpha) = \det(\sigma)\det\bigl(\delta(k)\bigr) = \pi(k).$$

Dies besagt, dass $k \in (K^*)'$, bzw., dass $\delta(k) \in \Sigma(P,H)'$ ist. Ist $|K| = 2$, so folgt $\delta(k) = 1$ und damit $\alpha = \sigma \in \mathrm{SL}(V)$. Ist $|K| > 2$, so ist $\mathrm{GL}(V)' = \mathrm{SL}(V)$ nach 2.7 a). Also gilt $\delta(k) \in \mathrm{SL}(V)$ und dann auch $\alpha \in \mathrm{SL}(V)$. Damit ist alles bewiesen.

Nun können wir endlich unser Versprechen einlösen.

3.6. Satz. *Ist V ein Vektorraum über dem Körper K und ist der Rang von V mindestens gleich 2, ist ferner P ein Punkt und H eine Hyperebene von $L_K(V)$ mit $V = P \oplus H$, so ist*

$$\mathrm{SL}(V) \cap \Sigma(P,H) = \Sigma(P,H)'.$$

Beweis. Dies ist richtig, falls $|K| = 2$ ist. Es sei also $|K| > 2$. Dann ist $\Sigma(P, H)' \subseteq \mathrm{SL}(V) \cap \Sigma(P, H)$, wie wir bereits wissen. Es sei $\delta(k) \in \mathrm{SL}(V) \cap \Sigma(P, H)$. Es gibt dann Transvektionen $\tau_1, \ldots, \tau_n$ mit

$$\delta(k) = \tau_1 \cdots \tau_n.$$

Es folgt

$$\pi(k) = \det\bigl(\delta(k)\bigr) = \pi(1)$$

ist. Also ist $k \in (K^*)'$ und damit $\delta(k) \in \Sigma(P, H)'$, so dass auch dieser Satz bewiesen ist.

Nach Cohn (1977, S. 117) gibt es nicht kommutative Körper, deren innere Automorphismengruppe auf $K^* - \{1\}$ transitiv operiert. Dies hat zur Folge, dass $(K^*)' = K^*$ ist. Ist V ein Vektorraum über einem solchen Körper, so ist nach unseren Entwicklungen also $\mathrm{GL}(V) = \mathrm{SL}(V)$.

Die hier konstruierte Funktion det stimmt im Falle endlich erzeugter Vektorräume mit der in der sonstigen Literatur det genannten Funktion überein, da die Einschränkungen beider Funktionen auf die Menge der Transvektionen und Dilatationen übereinstimmen (siehe etwa Lüneburg 1993).

4. Ausnahmeisomorphismen

Für diesen Abschnitt wird unterstellt, dass der Leser mit den Grundbegriffen der Theorie endlicher Gruppen vertraut ist. Unser Hauptziel ist, den folgenden Satz zu beweisen.

4.1. Satz. *Die folgenden Gruppen sind isomorph:*

a) $\mathrm{PSL}(2, 2)$ *und* S_3.

b) $\mathrm{PSL}(2, 3)$ *und* A_4.

c) $\mathrm{PSL}(2, 4)$, $\mathrm{PSL}(2, 5)$ *und* A_5 *(Hölder 1892).*

d) $\mathrm{PSL}(2, 7)$ *und* $\mathrm{PSL}(3, 2)$ *(Hölder 1892).*

e) $\mathrm{PSL}(2, 9)$ *und* A_6.

f) $\mathrm{PSL}(4, 2)$ *und* A_8. *(Jordan 1870/1989, S. 380 ff.)*

Um a) zu beweisen, hat man nur zu beachten, dass $\mathrm{PSL}(2, 2)$ eine Permutationsgruppe vom Grade 3 ist, die nach 1.13 die Ordnung 6 hat.

Um b) zu beweisen, bemerkt man, dass $\mathrm{PSL}(2, 3)$ eine Permutationsgruppe vom Grade 4 ist, die von Transvektionen erzeugt wird. Da die Transvektionen in diesem Falle 3-Zyklen sind, folgt, dass $\mathrm{PSL}(2, 3)$ zu einer Untergruppe der A_4 isomorph ist. Schließlich folgt aus 1.13, dass $|\mathrm{PSL}(2, 3)| = 12 = |A_4|$ ist. Dies zeigt, dass $\mathrm{PSL}(2, 3)$ und A_4 isomorph sind.

Um c) zu beweisen, bemerken wir zunächst, dass $\mathrm{PSL}(2, 4)$ eine einfache Permutationsgruppe vom Grade 5 ist. Da eine einfache Permutationsgruppe keine ungerade Permutation enthalten kann, folgt, dass $\mathrm{PSL}(2, 4)$ zu einer Untergruppe der A_5 isomorph ist. Wegen $|\mathrm{PSL}(2, 4)| = 60 = |A_5|$ folgt daher, dass $\mathrm{PSL}(2, 4)$ und A_5 isomorph sind. Damit ist eine der beiden Aussagen

von c) bewiesen. Darüber hinaus ist gezeigt, dass A_5 einfach ist. Nun ist $|\mathrm{PSL}(2,5)| = 60$ und $\mathrm{PSL}(2,5)$ ist einfach. Daher ist c) eine Konsequenz des folgenden allgemeineren Satzes.

4.2. Satz. *Es gibt bis auf Isomorphie nur eine einfache Gruppe der Ordnung* 60 *(Hölder 1892).*

Beweis. Es sei G eine einfache Gruppe der Ordnung 60. Enthält G eine Untergruppe vom Index 5, so besitzt G wegen der Einfachheit eine treue Darstellung vom Grade 5 und es folgt, dass G zur A_5 isomorph ist. Es ist also zu zeigen, dass G eine solche Untergruppe enthält. Dazu zeigen wir zunächst, dass G keine Untergruppe vom Index 3 enthält. Enthielte G eine solche Gruppe, so folgte aus der Einfachheit von G, dass G zu einer Untergruppe der S_3 isomorph wäre, was wegen $|G| = 60 > 6 = |S_3|$ nicht sein kann. Es seien S und T zwei verschiedene 2-Sylowgruppen von G. Ferner sei $1 \neq s \in S \cap T$. Die Ordnung einer 2-Sylowgruppe von G ist gleich 4. Daher sind S und T abelsch und es folgt, dass sie beide im Zentralisator C von S liegen. Daher gilt $|C| \geq 3 \cdot 4$. Weil G einfach ist, ist C von G verschieden. Also ist $|C| = 12$ oder 20. Weil G keine Untergruppe vom Index 3 besitzt, ist also $|C| = 12$, so dass C eine Untergruppe vom Index 5 ist. Wir dürfen daher annehmen, dass je zwei 2-Sylowgruppen von G trivialen Schnitt haben.

Es seien wieder S und T zwei verschiedene 2-Sylowgruppen von G. Ferner sei $s \in S$ und es gelte $s^{-1}Ts = T$. Dann erzeugen T und s eine 2-Gruppe, so dass $s \in T$ folgt. Auf Grund unserer Annahme ist daher $s = 1$. Hieraus folgt, dass die Anzahl der 2-Sylowgruppen von G kongruent 1 modulo 4 ist. Da diese Anzahl aber auch ein Teiler von $|G| = 60$ ist und wegen der Einfachheit von G nicht 1 sein kann, folgt, dass G genau fünf 2-Sylowgruppen hat, so dass der Normalisator einer solchen den Index 5 hat. Damit ist 4.2 bewiesen.

Da $|\mathrm{PSL}(2,7)| = 168 = |\mathrm{PSL}(3,2)|$ ist, folgt d) aus

4.3. Satz. *Es gibt bis auf Isomorphie nur eine einfache Gruppe der Ordnung* 168 *(Hölder 1892).*

Beweis. Es sei G eine einfache Gruppe der Ordnung $168 = 8 \cdot 3 \cdot 7$. Die Anzahl der 7-Sylowgruppen von G ist kongruent 1 modulo 7 und ein Teiler von 168. Überdies ist sie größer als 1, da G einfach ist. Es folgt, dass G genau acht 7-Sylowgruppen enthält. Es sei N der Normalisator einer solchen. Dann ist also $|N| = 3 \cdot 7$. Stellt man G dar als Permutationsgruppe auf der Menge der Rechtsrestklassen nach N, so ist diese Darstellung treu, da G einfach ist. Somit hat G eine Darstellung als transitive Gruppe von Grade 8. Der Stabilisator von N in dieser Darstellung ist N selber und hat daher die Ordnung 21. Hieraus folgt, dass G sogar zweifach transitiv ist.

Wir bezeichnen die Rechtsrestklassen von N mit P_∞, P_0, P_1, $\dots$, P_6, wobei wir annehmen, dass $N = P_\infty$ ist. Es sei σ ein Element der Ordnung 7 in N. Indem wir die P_i gegebenenfalls umnummerieren, können wir erreichen, dass $P_i^\sigma = P_{i+1}$ ist, wobei die Indizes modulo 7 zu reduzieren sind. Es sei $\nu \in N$. Dann ist $\nu^{-1}\sigma\nu = \sigma^a$ mit einer Zahl a, die zwischen 0 und 6 liegt. Definiere f

durch $P_i^\nu = P_{f(i)}$. Dann ist

$$P_{f(i+1)} = P_{i+1}^\nu = P_i^{\sigma\nu} = P^{\nu\sigma^a} = P_{f(i)+a}.$$

Also ist $f(i+1) = f(i)+a$. Setzt man $b := f(0)$, so erhält man, dass $f(i) = ai+b$ ist. Schließlich folgt aus $|N| = 21$, dass ν^3 in der von σ erzeugten Gruppe liegt. Dies impliziert wiederum die Kongruenz $a^3 \equiv 1 \bmod 7$. Hat ν zwei von P_∞ verschiedene Fixpunkte P_i und P_j, so ist $i \neq j$ und $i = ai + b$ sowie $j = aj + b$, woraus $a = 1$ und $b = 0$ folgt. Also induziert ν die Identität in $\{P_0, \ldots, P_\infty\}$, woraus $\nu = 1$ folgt, da G ja treu operiert. Damit ist gezeigt, dass N aus allen Abbildungen ν mit $P_\infty^\nu = P_\infty$ und $P_i^\nu = P_{ai+b}$ besteht, wobei $a, b \in \mathrm{GF}(7)$ und $a^3 = 1$ ist. Schließlich folgt noch, dass die Identität die einzige Permutation aus G ist, welche drei verschiedene der Punkte P_i festlässt.

Setze $K := \mathrm{GF}(7)$. Es sei $V = uK \oplus vK$ ein Vektorraum vom Rang 2 über K. Setzt man $P_\infty := vK$ und $P_i := (u + vi)K$, so wird G zu einer Permutationsgruppe auf der Menge der Punkte von $L_K(V)$. Ferner sieht man, dass die Gruppe, die von allen linearen Abbildungen λ der Form $u^\lambda = ua + vb$ und $v^\lambda = va^{-1}$ mit $a, b \in K$ und $a^3 = 1$ auf der Menge der Punkte von $L_K(V)$ induziert wird, gleich N ist. Wegen $\det(\lambda) = aa^{-1} = 1$ ist daher $N \subseteq \mathrm{PSL}(V)$.

Die 3-Sylowgruppen von G sind gerade die Stabilisatoren zweier Punkte aus $L_K(V)$. Weil die Identität die einzige Permutation aus G ist, die drei verschiedene Punkte festlässt, folgt, dass die Anzahl der 3-Sylowgruppen von G gleich $\binom{8}{2} = 28$ ist. Somit enthält G genau $2 \cdot 28 = 56$ Elemente der Ordnung 3. Ferner enthält G genau $8 \cdot 6 = 48$ Elemente der Ordnung 7.

Es seien nun P und Q zwei verschiedene Punkte von $L_K(V)$. Dann hat der Stabilisator H der Menge $\{P, Q\}$ die Ordnung 6 und die 3-Sylowgruppe S von H ist ein Normalteiler von H. Weil die Identität die einzige Permutation in G ist, die drei Fixpunkte hat, zerlegt S die Menge der von P und Q verschiedenen Punkte in zwei Bahnen der Länge 3. Da Involutionen keine Fixpunkte haben, werden diese beiden Bahnen von den in H liegenden Involutionen vertauscht, so dass H neben der Bahn $\{P, Q\}$ noch eine weitere Bahn der Länge 6 hat.

Wäre H zyklisch, so enthielte H genau zwei Elemente der Ordnung 6. An Hand der Bahnen von H sieht man, dass G dann mindestens $2 \cdot \binom{8}{2} = 56$ Elemente der Ordnung 6 enthielte. Da G, wie wir schon wissen, 56 Elemente der Ordnung 3 und 48 Elemente der Ordnung 7 enthält, enthielte G höchstens $168 - 2 \cdot 56 - 48 = 8$ Elemente, deren Ordnung eine Potenz von 2 ist. Folglich enthielte G nur eine 2-Sylowgruppe im Widerspruch zur Einfachheit von G. Also ist H nicht zyklisch und damit nicht abelsch.

Es sei jetzt insbesondere $P = P_0$ und $Q = P_\infty$. Dann induziert die durch $u^\rho := 2u$ und $v^\rho := 4v$ definierte Abbildung ρ ein Element der Ordnung 3 aus H. Die von ρ erzeugte Gruppe hat die beiden Bahnen $B_1 := \{P_1, P_2, P_4\}$ und $B_2 := \{P_{-1}, P_{-2}, P_{-4}\}$. Es sei λ eine Involution aus H. Wie wir gesehen haben, ist $B_1^\lambda = B_2$. Weil H als nicht abelsche Gruppe drei Involutionen enthält, dürfen wir annehmen, dass $P_1^\lambda = P_{-1}$ ist. Ist $i \neq 0$, so gibt es ein $g(i) \in K^*$ mit $P_i^\lambda = P_{g(i)}$. Weil H nicht zyklisch ist, ist $\rho\lambda = \lambda\rho^{-1}$. Also ist

$$P_{g(2i)} = P_i^{\rho\lambda} = P_i^{\lambda\rho^{-1}} = P_{4g(i)}.$$

Daher ist $g(2i) = 4g(i)$. Wegen $g(1) = -1$ ist daher $g(2) = -4$ und $g(4) = 4g(2) = -2$. Aus $\lambda^2 = 1$ folgt somit

$$\lambda = (P_0P_\infty)(P_1P_6)(P_2P_3)(P_4P_5).$$

definiert man die Abbildung κ durch $u^\kappa := -v$ und $v^\kappa := u$, so sieht man, dass $\kappa \in L_K(V)$ die Permutation λ induziert. Wegen $\det(\kappa) = 1$ ist daher $\lambda \in \mathrm{PSL}(V)$. Weil G das Erzeugnis von N und λ ist, folgt weiter $G \subseteq \mathrm{PSL}(V)$. Aus $|G| = 168 = |\mathrm{PSL}(V)|$ folgt schließlich die Behauptung.

Um e) zu beweisen, nutzen wir aus, dass die Gruppe $\mathrm{PSL}(2,9)$ eine zur A_5 isomorphe Untergruppe enthält. Dass dem so ist, folgt aus dem Satz, der besagt, dass $\mathrm{PSL}(2,q)$ genau dann eine zur A_5 isomorphe Untergruppe enthält, wenn $|\mathrm{PSL}(2,q)|$ durch 5 teilbar ist. Zum Beweise dieses Satzes müssen wir etwas weiter ausholen und beweisen zunächst den folgenden Satz (Moore 1897).

4.4. Satz. *Es sei m eine natürliche Zahl mit $m \geq 3$. Ist F die freie Gruppe in den Erzeugenden $a_1, \ldots, a_{m-2}$ und ist N der von den Elementen a_1^3, a_i^2 für $i := 2, \ldots, m-2$, $(a_ia_{i+1})^3$ für $i := 1, \ldots, m-3$ und $(a_ia_j)^2$ für $1 \leq i \leq j-2 \leq m-4$ erzeugte Normalteiler von F, so ist F/N zur alternierenden Gruppe A_m vom Grade m isomorph.*

Beweis. Dies ist gewiss richtig für $m = 3$. In diesem Falle ist F ja die von a_1 erzeugte unendliche zyklische Gruppe und N ist ihre Untergruppe vom Index 3. Andererseits hat die alternierende Gruppe vom Grade 3 die Ordnung 3.

Es sei also $m > 3$ und der Satz gelte für $m - 1$. Dann ist die von den Elementen $a_1N, \ldots, a_{m-3}N$ erzeugte Untergruppe U von F/N nach Induktionsannahme ein epimorphes Bild der A_{m-1}. Es folgt $|U| \leq \frac{1}{2}(m-1)!$. Es sei V die Untergruppe von F mit $V/N = U$. Dann gilt $a_i \in V$ für $i := 1, \ldots, m-3$. Wir definieren die Rechtsrestklassen R_i von V rekursiv durch $R_{m-1} := V$ und $R_i := R_{i+1}a_i$ für $i := m-2, \ldots, 1$ sowie $R_0 := R_1a_1$ und zeigen, dass dies bereits alle Rechtsrestklassen nach V sind.

Zunächst beachten wir, dass $R_iy = R_i$ ist für alle i und alle $y \in N$, da N ein in V enthaltener Normalteiler ist. Es ist $R_{m-1}a_1 = R_{m-1}$. Es sei $i \geq 4$ und es gelte $R_ia_1 = R_i$. Dann ist $R_{i-1}a_1 = R_ia_{i-1}a_1$. Wegen $i - 1 \geq 3$ ist $(a_1a_{i-1})^2 \in N$. Es gibt daher $y, z \in N$ mit $a_{i-1}a_1 = ya_1^{-1}a_{i-1} = za_1^2a_{i-1}$. Hieraus folgt

$$R_{i-1}a_1 = R_iza_1^2a_{i-1} = R_{i-1}.$$

Also gilt $R_ia_1 = R_i$ für alle $i \geq 3$. Nun ist $R_2a_1 = R_1$, $R_1a_1 = R_0$ und wegen $a_1^3 \in N$ ist $R_0a_1 = R_2$. Damit ist gezeigt, dass Multiplikation von rechts mit a_1 die R_i untereinander permutiert. Wir beachten ferner, dass die Rechtsmultiplikation mit a_1 auf den Indizes die Permutation (012) bewirkt.

Es sei $j > 1$. Ist $i > j + 1$, so ist a_j mit a_i modulo N vertauschbar, da in diesem Falle ja a_j^2, a_i^2, $(a_ja_i)^2 \in N$ ist. Daher folgt mit einer simplen Induktion

$$R_ia_j = R_{i-1}a_ia_j = R_{i-1}a_ja_i = R_{i-1}a_i = R_i$$

für $i := j+2, \ldots, m-1$. Es ist

$$R_ja_j = R_{j+1}$$

und
$$R_{j+1}a_j = R_j.$$

Es sei $j = 2$. Es ist a_1^3, a_2^3, $(a_1a_2)^3 \in N$. Es folgt
$$\begin{aligned} R_1a_2 &= R_2a_1a_2 = R_2a_2a_1^{-1}a_2a_1^{-1} \\ &= R_3a_1^2a_2a_1^2 = R_3a_2a_1^2 \\ &= R_2a_1^2 = R_0 \end{aligned}$$

und
$$\begin{aligned} R_0a_2 &= R_1a_1a_2 = R_1a_2a_1^{-1}a_2a_1^{-1} \\ &= R_0a_1^{-1}a_2a_1^{-1} = R_1a_2a_1^{-1} = R_1 \end{aligned}$$

Multiplikation von rechts mit a_2 permutiert also die R_i und bewirkt auf den Indizes die Permutation $(01)(23)$.

Es sei $j > 2$. Dann ist a_{j-1}^2, a_j^2, $(a_{j-1}a_j)^3 \in N$. Hiermit und mit dem bereits Bewiesenen folgt
$$\begin{aligned} R_{j-1}a_j &= R_ja_{j-1}a_j = R_ja_ja_{j-1}a_ja_{j-1} \\ &= R_{j+1}a_{j-1}a_ja_{j-1} = R_{j+1}a_ja_{j-1} \\ &= R_ja_{j-1} = R_{j-1}. \end{aligned}$$

Mittels Induktion folgt hieraus
$$R_ia_j = R_i$$
für $i := 2, \ldots, j-1$. Wegen $j > 2$ ist $(a_1a_j)^2 \in N$. Hieraus folgt, wenn man noch bemerkt, dass $2 \leq j-1$ ist,
$$R_1a_j = R_2a_1a_j = R_2a_ja_1^{-1} = R_2a_1^{-1} = R_0$$

und
$$R_0a_j = R_1a_1a_j = R_1a_ja_1^{-1} = R_0a_1^{-1} = R_1.$$

Multiplikation von rechts mit a_j permutiert also die R_i und bewirkt auf den Indizes die Permutation $(01)(j, j+1)$. Damit ist gezeigt, dass der Index von V in F höchstens gleich m ist. Also ist auch der Index von U in F/N höchstens gleich m. Daher ist
$$|F/N| \leq \frac{1}{2}(m-1)!m = |A_m|.$$

Setze $\alpha_1 := (012)$ und $\alpha_i := (01)(i, i+1)$ für $i := 2, \ldots, m-2$. Dann zeigt eine simple Induktion, dass A_m von $\{\alpha_i \mid i := 1, \ldots, m-2\}$ erzeugt wird. Ferner gelten die Relationen $\alpha_1^3 = 1, \alpha_i^2 = 1$ für $i := 2, \ldots, m-2$, $(\alpha_i\alpha_{i+1})^3 = 1$ für $i := 1, \ldots, m-2$ und $(\alpha_i\alpha_j)^2 = 1$ für $1 \leq i \leq j-2$. Hieraus folgt, dass es einen Epimorphismus π von F/N auf A_m gibt mit $\pi(a_iN) = \alpha_i$ für alle i. Somit enthält F/N mindestens $|A_m|$ Elemente, so dass $|F/N| = |A_m|$ ist. Dies impliziert schließlich, dass π ein Isomorphismus ist. Damit ist der Satz bewiesen.

4.5. Satz. *Ist G eine von $\{1\}$ verschiedene Gruppe und hat G Erzeugende a und b mit $a^5 = b^2 = (ab)^3 = 1$, so ist G zur A_5 isomorph.*

Beweis. Wir zeigen, dass G ein epimorphes Bild der A_5 ist. Hieraus folgt wegen der Einfachheit der A_5 und der Voraussetzung, dass $G \neq \{1\}$ ist, die Behauptung über G.

Wir setzen $\alpha_1 := ba^{-1}$, $\alpha_2 := (ba)b(ba)^{-1}$ und $\alpha_3 := \alpha_2 aba^3$. Dann ist

$$(\alpha_1\alpha_2^{-1}\alpha_3)^2 = a^{3\cdot 2} = a \quad \text{und} \quad \alpha_1 a = b,$$

so dass G auch von $\{\alpha_1, \alpha_2, \alpha_3\}$ erzeugt wird.

Es ist

$$\alpha_1^3 = (ba^{-1})^3 = ((ab)^{-1})^3 = 1.$$

Ferner ist $\alpha_2^2 = 1$, da α_2 zu b konjugiert ist.

Aus $(ab)^3 = 1$ folgt $bab = a^{-1}ba^{-1}$ und damit dann

$$\alpha_3 = baba^{-1}baba^3 = a^{-1}ba^{-3}ba^2.$$

Daher ist

$$\begin{aligned}\alpha_3^2 &= a^{-1}ba^{-3}ba^2a^{-1}ba^{-3}ba^2 = a^{-1}ba^2baba^2ba^2\\ &= a^{-1}bababa^2 = a^{-1}a^{-1}b^2a^2 = 1.\end{aligned}$$

Es ist

$$\begin{aligned}\alpha_1\alpha_2 &= a^{-1}baba^{-1}b = ba^{-2}ba^{-2}b = ba^{-3}(ab)a^{-2}b\\ &= (a^{-2}b)^{-1}(ab)a^{-2}b\end{aligned}$$

und daher $(\alpha_1\alpha_2)^3 = 1$.

Es ist $ba^{-1}b = aba$ und somit

$$(\alpha_2\alpha_3)^2 = aba^4ba^3 = aba^{-1}ba^3 = a^2ba^4.$$

Hiermit folgt dann

$$(\alpha_2\alpha_3)^3 = a^2ba^4aba^3 = 1.$$

Wegen $ba^4b = ba^{-1}b = aba$ erhalten wir

$$\alpha_1\alpha_3 = ba^{-1}baba^{-1}baba^3 = aba^3ba^2ba^3$$

und weiter

$$\begin{aligned}(\alpha_1\alpha_3)^2 &= aba^3ba^2ba^4ba^3ba^2ba^3 = aba^3ba^3ba^4ba^2ba^3\\ &= aba^3ba^4ba^3ba^3 = aba^4ba^4ba^3 = a^2ba^5ba^3 = 1.\end{aligned}$$

Wir haben gezeigt, dass die Gruppe G von $\{\alpha_1, \alpha_2, \alpha_3\}$ erzeugt wird und dass die Relationen $\alpha_1^3 = \alpha_2^2 = \alpha_3^2 = 1$ und $(\alpha_1\alpha_2)^3 = (\alpha_2\alpha_3)^3 = (\alpha_1\alpha_3)^2 = 1$ gelten. Mit 4.4 folgt daher, dass G ein epimorphes Bild der A_5 ist. Damit ist, wie eingangs bemerkt, der Satz bewiesen.

Satz 4.5 sagt nichts darüber, ob A_5 eine Präsentation der in diesem Satz beschriebenen Art hat. Dies ist jedoch leicht nachzuprüfen und wird außerdem aus dem gleich noch zu Beweisenden hervorgehen.

4.6. Satz. *Es sei K ein kommutativer Körper und V sei ein Vektorraum vom Rang 2 über K. Ist $\sigma \in \mathrm{SL}(V)$, so gilt:*
a) *Ist* $\mathrm{Spur}(\sigma) = 1$, *so ist* $\sigma^3 = -1$.
b) *Ist* $\mathrm{Spur}(\sigma) = -1$, *so ist* $\sigma^3 = 1$.
c) *Ist* $\mathrm{Spur}(\sigma) = 0$, *so ist* $\sigma^2 = -1$.

Beweis. Nach dem Satz von Cayley–Hamilton ist $\sigma^2 - \mathrm{Spur}(\sigma)\sigma + 1 = 0$, da ja $\det(\sigma) = 1$. Also gilt c). Wegen $\sigma^3 = -\mathrm{Spur}(\sigma)\sigma^2 - \sigma$ folgen auch die Behauptungen a) und b).

4.7. Satz. *Es sei K ein kommutativer Körper und α sei ein involutorischer Automorphismus von K. Ferner sei $V = uK \oplus vK$ ein Vektorraum vom Rang 2 über K und f sei die durch*

$$f(ua + vb, uc + vd) := a^\alpha c + b^\alpha d$$

definierte α-Semibilinearform auf V. Bezeichnet $\mathrm{SU}(V, f)$ *die Gruppe aller linearen Abbildungen $\sigma \in \mathrm{SL}(V, K)$ mit $f(x^\sigma, y^\sigma) = f(x, y)$ für alle x, $y \in V$, so gilt:*
a) *Die Gruppe* $\mathrm{SU}(V, f)$ *ist isomorph zur Gruppe aller Matrizen*

$$\begin{pmatrix} a & b \\ -b^\alpha & a^\alpha \end{pmatrix}$$

mit a, $b \in K$ und $a^{1+\alpha} + b^{1+\alpha} = 1$.
b) *Gibt es ein $x \in V - \{0\}$ mit $f(x, x) = 0$ und ist W ein Vektorraum vom Rang 2 über dem Fixkörper*

$$F := \{k \mid k \in K, k^\alpha = k\}$$

von α, so ist $\mathrm{SU}(V, f)$ *zu* $\mathrm{SL}(W, F)$ *isomorph.*

Beweis. a) Es sei $\sigma \in \mathrm{SL}(V, K)$. Es gibt dann Elemente a, b, c, $d \in K$ mit $u^\sigma = ua + vb$, $v^\sigma = uc + vd$ und $ad - bc = 1$. Nun liegt σ genau dann in $\mathrm{SU}(V, f)$, wenn

$$f(u^\sigma, u^\sigma) = 1 = f(v^\sigma, v^\sigma)$$

und

$$f(u^\sigma, v^\sigma) = 0$$

ist. Also liegt σ genau dann in $\mathrm{SU}(V, f)$, wenn

$$\begin{aligned} 1 &= a^{1+\alpha} + b^{1+\alpha}, \\ 1 &= c^{1+\alpha} + d^{1+\alpha}, \\ 0 &= a^\alpha c + b^\alpha d, \\ 1 &= ad - bc \end{aligned}$$

ist. Man verifiziert mühelos, dass diese Gleichungen genau dann erfüllt sind, wenn $d = a^\alpha$, $c = -b^\alpha$ und $a^{1+\alpha} + b^{1+\alpha} = 1$ ist. Damit ist a) bewiesen.

b) Aus $f(x,x) = 0$ und $x \neq 0$ folgt, dass $x \notin vK$ ist. Ist also $x = ur + vs$, so ist $r \neq 0$. Es folgt

$$f(x,u) = r^\alpha \neq 0.$$

Wir dürfen daher annehmen, dass $f(x,u) = 1$ ist.

Es gilt natürlich auch $x \notin uK$. Daher ist $V = xK \oplus uK$. Es sei $y := u + xr$. Dann ist

$$\begin{aligned} f(y,y) &= f(u+xr, u+xr) \\ &= f(u,u) + r^\alpha f(x,u) + rf(u,x) + r^{1+\alpha} f(x,x) \\ &= 1 + r + r^\alpha. \end{aligned}$$

Die durch $\varphi(r) := r + r^\alpha$ definierte Abbildung φ ist eine lineare Abbildung des F-Vektorraumes K in F. Wäre $\varphi = 0$, so wäre $r^\alpha = -r$ für alle $r \in K$. Es folgte $1 = 1^\alpha = -1$ und damit $r^\alpha = r$, so dass α die Identität wäre. Involutionen sind aber *per definitionem* von der Identität verschieden. Also ist φ nicht Null und damit surjektiv. Es gibt also ein $r \in K$ mit $1 + r + r^\alpha = 0$. Ist nun $y := u + xr$ mit eben diesem r, so ist $f(y,y) = 0$. Ferner ist

$$f(x,y) = f(x,u) + f(x,x)r = 1.$$

Es gibt ein $s \in K$ mit $s^\alpha \neq s$. Setze $k := s - s^\alpha$. Dann ist $k \neq 0$ und $k^\alpha = -k$. Setze $z := yk$. Dann ist $f(z,z) = 0$ und $f(x,z) = f(x,y)k = k = -f(z,x)$. Schließlich gilt $V = xK \oplus zK$, da ja $y \notin xK$ ist.

Es sei nun $\sigma \in \mathrm{SU}(V,f)$ und $x^\sigma = xa + zb$ sowie $z^\sigma = xc + zd$. Dann gelten die Gleichungen

$$\begin{aligned} 1 &= ad - bc, \\ 0 &= f(x,x) = f(x^\sigma, x^\sigma) = k(a^\alpha b - ab^\alpha), \\ 0 &= f(z,z) = f(z^\sigma, z^\sigma) = k(c^\alpha d - cd^\alpha), \\ k &= f(x,z) = f(x^\sigma, z^\sigma) = k(a^\alpha d - b^\alpha c). \end{aligned}$$

Weil $k \neq 0$ ist, gelten daher auch die Gleichungen

$$\begin{aligned} 1 &= ad - bc, \\ 0 &= a^\alpha b - ab^\alpha, \\ 0 &= c^\alpha d - cd^\alpha, \\ 1 &= a^\alpha d - b^\alpha c. \end{aligned}$$

Aus den beiden letzten Gleichungen sowie der ersten folgt

$$d^\alpha = (a^\alpha d^\alpha - b^\alpha c^\alpha)d = (ad - bc)^\alpha d = d$$

und

$$c^\alpha = (a^\alpha d^\alpha - b^\alpha c^\alpha)c = (ad - bc)^\alpha c = c.$$

Also liegen c und d in F. Aus der zweiten und vierten Gleichung folgt unter Benutzung der ersten

$$a = (ad - bc)a^\alpha = a^\alpha$$

und

$$b = (ad - bc)b^\alpha = b^\alpha.$$

Also liegen auch a und b in F. Sind umgekehrt a, b, c, $d \in F$ und ist $ad - bc = 1$, so verifiziert man ohne Mühe, dass die durch $x^\sigma := xa + zb$, $z^\sigma := xc + zd$ definierte Abbildung σ in $\mathrm{SU}(V, f)$ liegt. Damit ist gezeigt, dass $\mathrm{SU}(V, f)$ zur Gruppe aller Matrizen

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

mit a, b, c, $d \in F$ und $ad - bc = 1$ isomorph ist. Da diese Gruppe wiederum mit $\mathrm{SL}(W, F)$ isomorph ist, ist alles bewiesen.

4.8. Korollar. *Die Gruppe* $\mathrm{SL}(2, q)$ *ist isomorph zur Gruppe aller Matrizen*

$$\begin{pmatrix} a & b \\ -b^q & a^q \end{pmatrix}$$

mit a, $b \in \mathrm{GF}(q^2)$ *und* $a^{1+q} + b^{1+q} = 1$.

Beweis. Es sei $K := \mathrm{GF}(q^2)$ und $V = uK \oplus vK$ sei ein Vektorraum vom Rang 2 über K. Ferner sei f die durch

$$f(ua + vb, uc + vd) := a^q c + b^q d$$

definierte Semibilinearform auf V. Das Korollar 4.8 folgt aus 4.7, wenn wir nachweisen können, dass es einen Vektor $x \in V - \{0\}$ gibt mit $f(x, x) = 0$.

Die multiplikative Gruppe von K ist zyklisch und hat die Ordnung $q^2 - 1$. Daher ist die durch $r^\eta := r^{q+1}$ definierte Abbildung η ein Homomorphismus der multiplikativen Gruppe von K auf die multiplikative Gruppe von $\mathrm{GF}(q)$. Es gibt daher ein $r \in K$ mit $r^{1+q} = -1$. Setzt man $x := u + vr$, so ist $x \neq 0$ und $f(x, x) = 1 + r^{1+q} = 0$, so dass x die gewünschten Eigenschaften hat.

4.9. Satz. *Genau dann enthält* $\mathrm{PSL}(2, q)$ *eine zur* A_5 *isomorphe Untergruppe, wenn die Ordnung von* $\mathrm{PSL}(2, q)$ *durch* 5 *teilbar ist.*

Beweis. Die Notwendigkeit der Bedingung ist trivial. Es sei also 5 ein Teiler von $|\mathrm{PSL}(2, q)|$. Wir setzen $K := \mathrm{GF}(q)$ und $V = uK \oplus vK$ sei ein Vektorraum vom Range 2 über K. Wie wir wissen, ist

$$\bigl|\mathrm{PSL}(2, q)\bigr| = \frac{1}{\mathrm{ggT}(2, q - 1)} q(q^2 - 1).$$

Drei Fälle sind zu unterscheiden.

1. Fall: Es ist $q = 5^r$. Betrachtet man die Menge aller Abbildungen σ der Form $u^\sigma = ua + vb$ und $v^\sigma = uc + vd$ mit a, b, c, $d \in \mathrm{GF}(5)$ und $ad - bc = 1$, so ist diese eine zur $\mathrm{SL}(2, 5)$ isomorphe Untergruppe von $\mathrm{SL}(2, q)$. Hieraus folgt, dass $\mathrm{PSL}(2, q)$ eine zur $\mathrm{PSL}(2, 5)$ isomorphe Untergruppe enthält. Da diese nach 4.1c) zur A_5 isomorph ist, gilt in diesem Falle die Behauptung.

2. Fall: Es ist 5 ein Teiler von $q - 1$. In diesem Falle gibt es ein $a \in K$ mit $a^5 = 1 \neq a$. Es folgt $a - a^{-1} \neq 0$. Wir setzen $b := (a - a^{-1})^{-1}$ und wählen c,

$d \in K$, so dass $b^2+cd = -1$ ist. Wir definieren die Abbildungen σ und τ von V in sich durch $u^\sigma := ua$ und $v^\sigma := va^{-1}$ sowie $u^\tau := ub+vc$ und $v^\tau := ud-vb$. Dann ist zunächst $\det(\sigma) = 1 = \det(\tau)$. Ferner ist $\sigma^5 = 1$ und $\mathrm{Spur}(\tau) = b - b = 0$, so dass nach 4.6b) also $\tau^2 = -1$ ist. Schließlich ist $u^{\sigma\tau} = uba + vca$ und $v^\sigma\tau = uda^{-1} - vba^{-1}$ und daher $\mathrm{Spur}(\sigma\tau) = b(a - a^{-1}) = 1$, so dass nach 4.6a) die Gleichung $(\sigma\tau)^{-3} = -1$ gilt. Sind $\bar\sigma$ und $\bar\tau$ die von σ und τ in $\mathrm{PSL}(2,q)$ induzierten Abbildungen, so ist also $\bar\sigma \neq 1$ und $\bar\sigma^5 = \bar\tau^2 = (\bar\sigma\bar\tau)^3 = 1$, so dass nach 4.5 die von $\bar\sigma$ und $\bar\tau$ erzeugte Untergruppe von $\mathrm{PSL}(2,q)$ zur A_5 isomorph ist.

3. Fall: Es ist 5 ein Teiler von $q+1$. Es gibt ein $a \in \mathrm{GF}(q^2)$ mit $a^5 = 1 \neq a$. Weil 5 ein Teiler von $q+1$ ist, folgt $a^{1+q} = 1$. Da $q-1$ nicht durch 5 teilbar ist, ist $a^q \neq a$. Wir setzen $b := (a-a^q)^{-1}$. Dann ist $b^q = -b$ und folglich $1 - b^{1+q} \in K$, so dass es ein $c \in \mathrm{GF}(q^2)$ gibt mit $c^{1+q} = 1 - b^{1+q}$. Wir betrachten die Matrizen

$$A := \begin{pmatrix} a & 0 \\ 0 & a^q \end{pmatrix} \quad \text{und} \quad B := \begin{pmatrix} b & c \\ -c^q & b^q \end{pmatrix}.$$

Dann ist $\det(A) = a^{1+q} = 1 = b^{1+q} + c^{1+q} = \det(B)$. Ferner ist $a^5 = 1$ und $\mathrm{Spur}(B) = b + b^q = b - b = 0$, so dass $B^2 = 1$ ist. Schließlich ist $\mathrm{Spur}(AB) = b(a - a^q) = 1$, woraus $(AB)^3 = -1$ folgt. Aus 4.8 und 4.5 folgt daher, dass $\mathrm{PSL}(2,q)$ auch in diesem Falle eine zur A_5 isomorphe Untergruppe enthält. Damit ist 4.9 bewiesen.

Um 4.1 e) zu beweisen, beachten wir zunächst, dass $|\mathrm{PSL}(2,9)| = 360 = |A_6|$ ist. Nach 4.9 enthält $\mathrm{PSL}(2,9)$ eine zur A_5 isomorphe Untergruppe, so dass sie, da sie einfach ist, eine treue Darstellung als Permutationsgruppe vom Grad 6 besitzt. Wiederum wegen der Einfachheit kann sie nur gerade Permutationen enthalten, so dass sie zu einer Untergruppe der A_6 isomorph ist. Aus der Gleichheit der Ordnungen folgt daher die Isomorphie der Gruppen.

Es bleibt zu zeigen, dass die Gruppen $\mathrm{PSL}(4,2)$ und A_8 isomorph sind. Es gibt mehrere Möglichkeiten, dies zu beweisen. Der schönste Beweis scheint mir der von Moore zu sein, der hier wiedergegeben sei (Moore 1899).

Wir betrachten das folgende Schema:

$$\begin{array}{ccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 \\ 3 & 4 & 5 & 6 & 0 & 1 & 2 \end{array}$$

Nennt man die Ziffern 0 bis 6 Punkte und die Ziffernmengen, die aus den Ziffern einer Spalte bestehen, Geraden und definiert man die Inzidenz als die $\in$-Relation, so ist die so entstehende Inzidenzstruktur die projektive Ebene der Ordnung 2. Aus dem zweiten Struktursatz und Satz 1.13 folgt, dass $\mathrm{PSL}(3,2)$ die volle Kollineationsgruppe dieser Ebene ist. Weil diese Gruppe einfach ist, ist sie eine Untergruppe der A_7. Mit 1.13 folgt, dass ihr Index in der A_7 gleich 15 ist. Hieraus folgt, dass die Wirkung der A_7 auf der Menge $\{0,\ldots,6\}$ insgesamt 15 verschiedene Realisierungen der projektiven Ebene der Ordnung 2 liefert. Diese nennen wir Punkte einer Geometrie Σ, deren Geraden die 3-Teilmengen von $\{0,\ldots,6\}$ sind. (Ziffern heißen im Folgenden wieder Ziffern.)

Wir definieren Inzidenz dadurch, dass für einen Punkt P und eine Gerade G von Σ genau dann $P \mathrel{\mathrm{I}} G$ gelte, wenn G eine Gerade der projektiven Ebene P ist. Wir werden zeigen, dass Σ aus den Punkten und Geraden des projektiven Raumes des Ranges 4 über GF(2) besteht.

1) Σ enthält $v = 15$ Punkte und $b = 35$ Geraden und jeder Punkt inzidiert mit genau $r = 7$ Geraden.

Dies folgt unmittelbar aus der Definition von Σ.

2) A_7 operiert als Automorphismengruppe auf Σ und ist sowohl auf der Menge der Punkte als auch auf der Menge der Geraden von Σ transitiv.

Auch dies ist eine unmittelbare Konsequenz aus der Definition von Σ.

3) Jede Gerade von Σ trägt genau drei Punkte.

Aus 2) folgt, dass jede Gerade mit gleich vielen, etwa k Punkten inzidiert. Das beim Beweise von I.7.5 benutzte Verfahren der zweifachen Abzählung liefert im vorliegenden Falle die Gleichung $vr = bk$, dh. die Gleichung $15 \cdot 7 = 35 \cdot k$, so dass in der Tat $k = 3$ ist.

4) Zwei verschiedene Geraden G und H haben genau dann einen Punkt gemeinsam, wenn sie als Tripel genau eine Ziffer gemeinsam haben.

Liegt der Punkt Q auf den beiden Geraden G und H, so sind die Tripel G und H Geraden der projektiven Ebene Q, so dass sie genau eine Ziffer gemeinsam haben. Haben sie umgekehrt genau eine Ziffer gemeinsam, so ist $|G \cup H| = 5$. Weil die A_7 auf $\{0, \ldots, 6\}$ fünffach transitiv ist, können wir annehmen, dass $G = \{0, 1, 3\}$ und $H = \{1, 2, 4\}$ ist. Dann sind G und H aber Geraden der Ebene, von der wir ausgegangen sind, so dass sie als Geraden von Σ einen Punkt gemeinsam haben.

5) Zwei verschiedene Geraden haben höchstens einen Punkt gemeinsam.

Es seien G und H zwei Geraden, die einen Punkt Q gemeinsam haben. Nach 4) ist dann $|G \cup H| = 1$. Weil die Kollineationsgruppe K der projektiven Ebene Q auf den Rahmen dieser Ebene transitiv ist, ist sie erst recht auf der Menge der 2-Teilmengen der Geradenmenge transitiv. Da es sieben Geraden gibt, hat diese Menge die Länge 21. Daher gilt für den Stabilisator $K_{\{G,H\}}$ der Menge $\{G, H\}$, dass

$$|K_{\{G,H\}}| = |K|/21 = 168/21 = 8$$

ist. Da die Menge aller 2-Teilmengen von Tripeln mit genau einer gemeinsamen Ziffer gleich

$$\frac{1}{2} \cdot 7 \cdot \binom{6}{2} \cdot \binom{4}{2} = 7 \cdot 3^2 \cdot 5$$

ist, folgt $\left|(A_7)_{\{G,H\}}\right| = 8$, so dass $K_{\{G,H\}} = (A_7)_{\{G,H\}}$ ist. Hieraus folgt, dass es außer Q keinen weiteren Punkt mehr gibt, der auf G und auf H liegt.

6) Durch zwei verschiedene Punkte geht genau eine Gerade.

Sind Pund Q zwei verschiedene Punkte, so bezeichnen wir mit $r_{\{P,Q\}}$ die Anzahl der mit P und Q gleichzeitig inzidierenden Geraden. Mit 5) folgt, dass $r_{\{P,Q\}} \leq 1$ ist. Da die Anzahl der 2-Teilmengen von Punkten, die auf einer

Geraden liegen, gleich 3 ist, liefert zweifache Abzählung

$$35 \cdot 3 = \sum_{\{P,Q\}} r_{\{P,Q\}} \leq \binom{15}{2} = 15 \cdot 7.$$

Hieraus folgt die Behauptung.

Es bleibt, die Gültigkeit des Veblen-Young-Axioms nachzuweisen. Dazu seien P, Q und R drei nicht kollineare Punkte von Σ. Ferner seien D und E zwei verschiedene Punkte mit $D \mathrel{\mathrm{I}} P + Q$ und $E \mathrel{\mathrm{I}} Q + R$. Wir haben zu zeigen, dass die Geraden $D+E$ und $R+P$ einen Punkt gemeinsam haben. Wir dürfen wieder annehmen, dass $P + Q = \{0, 1, 3\}$ und $Q + R = \{1, 2, 4\}$ ist. Die Gerade $R+P$ hat mit den beiden Geraden $P+Q$ und $Q+R$ jeweils genau eine Ziffer gemeinsam. Wäre $1 \in R + P$, so wäre daher $R + P = \{1, 5, 6\}$. Da dies ein Tripel der Ebene Q ist, wären P, Q und R kollinear. Dieser Widerspruch zeigt, dass $1 \notin R + P$ ist. Indem wir nun gegebenenfalls eine der Permutationen $(03)(24), (03)(56)$ oder $(24)(56)$ anwenden, können wir erreichen, dass $0,\ 2 \in R + P$ ist. Also ist $R + P = \{0, 2, 5\}$ oder $R + P = \{0, 2, 6\}$. Wäre $R+P = \{0, 2, 6\}$, so wären P, Q und R aber kollinear. Also ist $R+P = \{0, 2, 5\}$.

Die Ziffernmenge $D+E$ hat mit $P+Q = \{0, 1, 3\}$ und $Q+R = \{1, 2, 4\}$ jeweils genau eine Ziffer gemeinsam. Daher ist $D + E$ gleich einem der neun Tripel $\{1, 5, 6\}$, $\{0, 2, x\}$, $\{0, 4, x\}$, $\{3, 2, x\}$, $\{3, 4, x\}$, wobei $x = 5$ oder 6 ist. Hätten nun $D + E$ und $R + P$ keinen Punkt gemeinsam, so folgte $D + E = \{0, 2, 6\}$, $\{0, 4, 5\}$, $\{3, 2, 5\}$, $\{3, 4, 6\}$. In jedem Falle folgte $Q \mathrel{\mathrm{I}} D + E$. Dann wäre aber entweder $Q = D$ und dann $D + E = Q + R$ oder $Q = E$ und $D + E = P + Q$, was beides nicht der Fall ist. Dieser Widerspruch zeigt, dass $D + E$ und $R + Q$ doch einen Punkt gemeinsam haben. Damit ist gezeigt, dass Σ eine projektive Geometrie ist.

Da auf jeder Geraden von Σ genau drei Punkte liegen, ist die Ordnung von Σ gleich 2. Ist r der Rang der Geometrie, so ist also $15 = 2^r - 1$, so dass $r = 4$ ist. Auf Grund des ersten Struktursatzes ist Σ daher die projektive Geometrie vom Range 4 über $\mathrm{GF}(2)$. Von dieser wissen wir nun, dass sie eine Kollineationsgruppe besitzt, die zur A_7 isomorph ist. Aus Satz 1.13 folgt, dass

$$|\mathrm{P\Gamma L}(4, 2)| = |\mathrm{PGL}(4, 2)| = |\mathrm{PSL}(4, 2)| = |A_8|$$

ist. Ferner enthält $\mathrm{PSL}(4, 2)$, wie gerade gesehen, eine zur A_7 isomorphe Untergruppe. Diese hat natürlich den Index 8 in $\mathrm{PSL}(4, 2)$, so dass $\mathrm{PSL}(4, 2)$ auf den Rechtsrestklassen dieser Untergruppe als Permutationsgruppe vom Grade 8 operiert. Da die $\mathrm{PSL}(4, 2)$ einfach ist, folgt, dass sie in der alternierenden Gruppe vom Grade 8 enthalten ist. Weil beide Gruppen die gleiche Ordnung haben, sind sie also gleich.

Damit ist Satz 4.1 vollständig bewiesen. Zum Schluss haben wir mehr bewiesen als in diesem Satze formuliert. Es ist also noch ein Korollar zu formulieren.

4.10. Korollar. *Ist V der Vektorraum vom Range 4 über $\mathrm{GF}(2)$, so besitzt $\mathrm{PSL}(V)$ eine zur A_7 isomorphe Kollineationsgruppe, die auf den Punkten von $L_{\mathrm{GF}(2)}(V)$ zweifach transitiv operiert.*

Beweis. Die A_7 operiert in obiger Darstellung auf der Menge der Geraden transitiv. Wir setzen $\gamma := (456)$ und bezeichnen mit P die Ebene, mit der wir starteten. Dann ist $P \neq P^\gamma \neq P^{\gamma^2} \neq P$. Folglich permutiert die von γ erzeugte Gruppe die mit der Geraden $\{0, 1, 2\}$ inzidierenden Punkte transitiv. Weil zwei verschiedene Punkte mit genau einer Geraden inzidieren, ist A_7 daher auf der Menge der 2-Teilmengen der Punktmenge transitiv. Weil die Ordnung der A_7 gerade ist, folgt schließlich, dass A_7 auf der Punktmenge der betrachteten Geometrie zweifach transitiv operiert.

Bei diesen Untersuchungen ist als Nebenergebnis herausgekommen, dass die Gruppen A_5, A_6 und A_8 einfach sind. Generell gilt, dass A_n einfach ist, wenn nur $n \neq 4$ ist. Dies beweist Camille Jordan in seinem *Traité* (Jordan 1870/1989, S. 66). Mit diesem Buche beginnen auch die systematischen Untersuchungen der in diesem Kapitel betrachteten und anderer in der Geometrie vorkommenden Gruppen, wobei Jordan als Körper nur die Galoisfelder $\mathrm{GF}(p)$ betrachtet, wo p eine Primzahl ist. Jordan kannte den Begriff der Faktorgruppe noch nicht, der erst durch Otto Hölder eingeführt wurde (Hölder 1889). Bei ihm, Jordan, findet sich die Einfachheit der $\mathrm{PSL}(n,p)$ unter dem Satz verborgen, dass ein Normalteiler der Gruppe $\mathrm{GL}(n,p)$ entweder im Zentrum von $\mathrm{GL}(n,p)$ enthalten ist oder aber die $\mathrm{SL}(n,p)$ enthält.

5. Quasiperspektivitäten

In diesem Abschnitt werden wir Kollineationen untersuchen, die eine Verallgemeinerung der Perspektivitäten darstellen und wie diese gewisse Unterraumkonfigurationen punktweise festlassen. Da sie sich also quasi wie Perspektivitäten verhalten, werden wir sie Quasiperspektivitäten nennen. Wir beginnen mit der Formulierung eines Satzes, der eine banale, jedoch sehr nützliche Folgerung aus Satz 1.2 ist.

5.1. Satz. *Es sei V ein Vektorraum über dem Körper K mit $\mathrm{Rg}_K(V) \geq 2$. Ist $\gamma \in \mathrm{P\Gamma L}(V)$ und lässt γ eine Gerade von $L_K(V)$ punktweise fest, so ist γ projektiv.*

Beweis. Es sei G eine Gerade von $L_K(V)$, die von γ punktweise festgelassen wird. Ferner sei $\delta \in \Gamma\mathrm{L}(V)$ und γ werde von δ induziert. Nach 1.2 gibt es dann ein $k \in K^*$ mit $g^\delta = gk$ für alle $g \in G$. Für den begleitenden Automorphismus α von δ gilt dann $x^\alpha = k^{-1}xk$, so dass α ein innerer Automorphismus ist. Nach 1.3 ist γ daher projektiv.

Es sei V ein Vektorraum über dem Körper K und τ sei eine Kollineation von $L_K(V)$, die einen Unterraum U festlässt. Dann induziert τ eine Kollineation τ^* in U und eine Kollineation τ^{**} in V/U. Wir nennen τ *Quasiperspektivität*, falls $\tau^* = 1$ und $\tau^{**} = 1$ ist. Ist τ eine Quasiperspektivität und ist $U = \{0\}$ oder $U = V$, so ist $\tau = 1$. Ist $\mathrm{Rg}_K(U) = 1$, so ist τ eine Perspektivität mit dem Zentrum U, und ist $\mathrm{Rg}_K(V/U) = 1$, so ist τ eine Perspektivität mit der Achse U. Es sei daher $\mathrm{Rg}_K(U) \geq 2$ und $\mathrm{Rg}_K(V/U) \geq 2$. Nach 5.1 ist τ projektiv. Es gibt daher eine lineare Abbildung σ, die τ induziert. Wegen $\mathrm{Rg}_K(U) \geq 2$ folgt

aus 1.2 die Existenz eines von Null verschiedenen Elementes m in $Z(K)$ mit $u^\sigma = um$ für alle $u \in U$. Wir können ohne Einschränkung der Allgemeinheit annehmen, dass $m = 1$ ist. Wegen $\mathrm{Rg}_K(V/U) \geq 2$ folgt fernerhin die Existenz eines von Null verschiedenen Elementes $k \in Z(K)$ mit $v^\sigma + U = vk + U$ für alle $v \in V$. Definiert man α durch $v^\alpha := v^\sigma - vk$ für alle $v \in V$, so ist α eine lineare Abbildung von V in U. Es sind nun zwei Fälle zu unterscheiden, nämlich die Fälle $k \neq 1$ und $k = 1$.

Ist $k \neq 1$, so nennen wir τ eine *Quasistreckung*. In diesem Falle setzen wir

$$W := \big\{v - v^\alpha(1-k)^{-1} \mid v \in V\big\}.$$

Dann ist W ein Unterraum von V, da k ja ein Zentrumselement ist. Aus $v^\alpha \in U$ und

$$v = v^\alpha(1-k)^{-1} + v - v^\alpha(1-k)^{-1}$$

folgt $V = U + W$. Ist $u \in U$, so ist $u^\alpha = u^\sigma - uk = u(1-k)$. Wegen $v^\alpha \in U$ ist daher

$$v^{\alpha^2} = v^\alpha(1-k).$$

Hiermit folgt

$$\big(v - v^\alpha(1-k)^{-1}\big)^\alpha = v^\alpha - v^\alpha(1-k)(1-k)^{-1} = 0.$$

Dies besagt, dass W im Kern von α liegt. Ist nun $x \in U \cap W$, so ist also $0 = x^\alpha = x(1-k)$, so dass $x = 0$. Folglich ist $V = U \oplus W$. Ferner ist

$$\begin{aligned}
\big(v - v^\alpha(1-k)^{-1}\big)^\sigma &= v^\sigma - v^{\alpha\sigma}(1-k)^{-1} \\
&= v^\sigma - v^\alpha(1-k)^{-1} \\
&= v^\alpha + vk - v^\alpha(1-k)^{-1} \\
&= \big(v^\alpha(1-k) + vk(1-k) - v^\alpha\big)(1-k)^{-1} \\
&= \big(vk(1-k) - v^\alpha k\big)(1-k)^{-1} \\
&= \big(v - v^\alpha(1-k)^{-1}\big)k.
\end{aligned}$$

Daher ist $w^\sigma = wk$ für alle $w \in W$. Die Kollineation τ lässt also in diesem Falle die beiden windschiefen Unterräume U und W punktweise fest, was den Namen Quasistreckung rechtfertigt.

Im Falle $k = 1$ gilt

$$v^{\alpha^2} = v^{\alpha\sigma} - v^\alpha k = v^\alpha - v^\alpha = 0,$$

da ja $v^\alpha \in U$ ist. Folglich ist $\alpha^2 = 0$. Ferner ist $u^\alpha = u^\sigma - u = u - u = 0$ für alle $u \in U$. Also ist $U^\alpha \subseteq U \subseteq \mathrm{Kern}(\alpha)$. Es sei $v^\sigma = va \neq 0$. Dann ist $va = v^\sigma = v + v^\alpha$. Hieraus folgt $v(a-1) = v^\alpha \in U$. Wäre $a \neq 1$, so wäre $v \in U$ und daher $v = v^\sigma = va$ und also doch $a = 1$. Also ist $v = v^\sigma = v + v^\alpha$ und damit $v^\alpha = 0$. Somit ist $v \in \mathrm{Kern}(\alpha)$. Dies besagt wiederum, dass τ außerhalb $\mathrm{Kern}(\alpha)$ keinen Fixpunkt hat. Deshalb nennen wir τ eine *Quasielation*. Ferner nennen wir $\mathrm{Kern}(\alpha)$ *Achse* und V^α *Zentrum* von τ.

5.2. Satz. *Es sei V ein Vektorraum über dem Körper K mit $\mathrm{Rg}_K(V) \geq 3$. Ferner seien U und W Unterräume von V mit $V = U \oplus W$. Schließlich bezeichne $\Lambda(U,W)$ die Gruppe aller Quasistreckungen, die U und W punktweise festlassen.*
a) *Ist $\mathrm{Rg}_K(U) = 1$ oder $\mathrm{Rg}_K(W) = 1$, so ist $\Lambda(U,W)$ zu K^* isomorph.*
b) *Ist $\mathrm{Rg}_K(U) \geq 2$ und $\mathrm{Rg}_K(W) \geq 2$, so ist $\Lambda(U,W)$ zu $Z(K^*)$ isomorph.*
In jedem Falle ist $\Lambda(U,W) \subseteq \mathrm{PG}^*\mathrm{L}(V)$.

Beweis. a) ist nichts Neues. Es ist hier nur noch einmal notiert, um den Kontrast zu b) deutlich werden zu lassen.

b) Ist $k \in Z(K^*)$ und definiert man $\lambda(k)$ durch

$$(u + w)^{\lambda(k)} := u + wk,$$

so induziert $\lambda(k)$ eine Kollineation aus $\Lambda(U,W)$. Wie wir schon gesehen haben, erhält man auf diese Weise alle Abbildungen aus $\Lambda(U,W)$. Mit 1.2 folgt, dass $\lambda(k)$ genau dann die Identität induziert, wenn $k = 1$ ist. Da λ offensichtlich ein Homomorphismus ist, ist bereits alles gezeigt.

Es sei wieder $V = U \oplus W$. Die Geometrie $L_K(V)$ werde (U,W)-*transitiv* genannt, falls es zu zwei verschiedenen Punkten P und Q, die weder auf U noch auf W liegen und für die $U \cap (P+Q) \neq \{0\}$ sowie $W \cap (P+Q) \neq \{0\}$ gilt, stets ein $\lambda \in \Lambda(U,W)$ gibt mit $P^\lambda = Q$.

5.3. Satz. *Ist V ein Vektorraum über dem Körper K mit $\mathrm{Rg}_K(V) \geq 4$, so sind die folgenden Aussagen äquivalent:*
a) *$L_K(V)$ ist papposch.*
b) *Sind $U, W \in L_K(V)$, ist $\mathrm{Rg}_K(U) \geq 2$ und $\mathrm{Rg}_K(W) \geq 2$ und ist $V = U \oplus W$, so ist $L_K(V)$ ein (U,W)-transitiver Raum.*
c) *Es gibt zwei Unterräume U, $W \in L_K(V)$ mit $\mathrm{Rg}_K(U) \geq 2$, $\mathrm{Rg}_K(W) \geq 2$ und $V = U \oplus W$, so dass $L_K(V)$ ein (U,W)-transitiver Raum ist.*

Beweis. a) impliziert b): Gilt a), so ist K kommutativ. Es sei $V = U \oplus W$. Ferner seien $P = pK$ und $Q = qK$ Punkte, die weder in U noch in V liegen, für die jedoch $(P+Q) \cap U \neq \{0\}$ und $(P+Q) \cap V \neq \{0\}$ gilt. Es gibt dann von 0 verschiedene Vektoren u, $u' \in U$ und w, $w' \in W$ mit $p = u + w$ und $q = u' + w'$. Weil $(P+Q) \cap U$ und $(P+Q) \cap W$ Punkte sind, gibt es von 0 verschiedene Elemente a, $b \in K$ mit $u' = ua$ und $w' = wb$. Setzt man $c := ba^{-1}$ und definiert σ durch $(x+y)^\sigma := x + yc$ für alle $x \in U$ und alle $y \in W$, so induziert σ wegen der Kommutativität von K eine Kollineation, die zu $\Lambda(U,W)$ gehört. Ferner ist

$$p^\sigma = u + vc = (ua + vb)a^{-1} = qa^{-1}$$

und daher $P^\sigma = Q$. Damit ist b) aus a) hergeleitet.

b) impliziert c): Natürlich, denn wir haben ja $\mathrm{Rg}_K(V) \geq 4$ vorausgesetzt.

c) impliziert a): Es sei $0 \neq u \in U$, $0 \neq w \in W$ und $0 \neq c \in K$. Dann sind $P := (u+w)K$ und $Q := (u+wc)K$ zwei verschiedene Punkte, die weder auf U noch auf W liegen und für die $(P+Q) \cap U = uK$ und $(P+Q) \cap W = wK$ gilt. Nach Voraussetzung gibt es ein $a \in Z(K^*)$, so dass die durch $(x+y)^\sigma := x + ya$

für alle $x \in U$ und alle $y \in W$ definierte Abbildung σ den Punkt P auf den Punkt Q abbildet. Es gibt daher ein $b \in K$ mit

$$u + wa = p^\sigma = qb = (u + wc)b.$$

Weil u und w linear unabhängig sind, folgt $b = 1$ und $a = c$, so dass $c \in Z(K)$ gilt. Daher ist K kommutativ, so dass $L_K(V)$ pappossch ist.

5.4. Satz. *Es sei V ein Vektorraum über dem Körper K und es gelte $\mathrm{Rg}_K(V) \geq 3$. Ferner seien U und W von $\{0\}$ verschiedene Unterräume von V mit $V = U \oplus W$. Schließlich sei Λ_1 die Gruppe aller Kollineationen aus $\mathrm{PG^*L}(V)$, die U als Ganzes und W punktweise festlassen, und Λ_2 die Gruppe aller Kollineationen aus $\mathrm{PG^*L}(V)$, die U punktweise und W als Ganzes festlassen. Dann gilt:*
a) *Die Gruppen Λ_1 und Λ_2 normalisieren sich gegenseitig.*
b) *Es ist $\Lambda_1 \cap \Lambda_2 = \Lambda(U, W)$.*
c) *Λ_1 induziert in $L_K(U)$ die Gruppe $\mathrm{PG^*L}(U)$ und Λ_2 induziert in $L_K(W)$ die Gruppe $\mathrm{PG^*L}(W)$.*
d) *$\Lambda_1\Lambda_2$ ist die Untergruppe aller Kollineationen aus $\mathrm{PG^*L}(V)$, die U und W festlassen.*
e) *Es ist $(\Lambda_1\Lambda_2)/\Lambda(U, W) \cong \mathrm{PG^*L}(U) \times \mathrm{PG^*L}(W)$.*
f) *Es ist $Z(\Lambda_1\Lambda_2) = Z(\Lambda(U, W))$.*

Beweis. a) und b) sind banal.

c) Wir zeigen, dass Λ_1 in $L_K(U)$ die Gruppe $\mathrm{PG^*L}(U)$ induziert. Die zweite Aussage beweist sich analog.

Weil λ_1 den Raum U festlässt, induziert Λ_1 eine Kollineationsgruppe L in $L_K(U)$, die in $\mathrm{PG^*L}(U)$ enthalten ist, da Λ_1 nur aus projektiven Kollineationen besteht. Es sei $\sigma \in \mathrm{PG^*L}(U)$. Es gibt dann ein $\lambda \in \mathrm{G^*L}(U)$, welches σ induziert. Wir definieren die Abbildung $\mu \in \mathrm{G^*L}(V)$ durch $(u + w)^\mu = u^\lambda + w$ für alle $u \in U$ und alle $w \in W$. Dann induziert μ eine Kollineation aus Λ_1, die auf $L_K(U)$ mit σ übereinstimmt. Also ist $L = \mathrm{PG^*L}(U)$.

d) Es sei γ eine projektive Kollineation mit $U^\gamma = U$ und $W^\gamma = W$. Nach c) gibt es ein $\lambda \in \Lambda_1$ mit $P^\gamma = P^\lambda$ für alle Punkte P von $LK(U)$. Es folgt $\gamma\lambda^{-1} \in \Lambda_2$ und damit $\gamma \in \Lambda_2\Lambda_1 = \Lambda_1\Lambda_2$.

e) Aus a) und b) folgt

$$(\Lambda_1\Lambda_2)/\Lambda(U, W) = \big(\Lambda_1/\Lambda(U, W)\big) \times \big(\Lambda_2/\Lambda(U, W)\big),$$

woraus mit c) die Behauptung folgt.

f) Es sei $\zeta \in Z(\Lambda_1\Lambda_2)$. Da $Z(\mathrm{PG^*L}(U)) = \{1\}$ und $Z(\mathrm{PG^*L}(W)) = \{1\}$ ist, folgt mit c), dass $\zeta \in \Lambda(U, W)$ gilt. Somit ist $Z(\Lambda_1\Lambda_2) \subseteq Z(\Lambda(U, W))$.

Es sei umgekehrt $\zeta \in Z(\Lambda(U, W))$: Dann gibt es ein $k \in Z(K^*)$ mit $(u + w)^\zeta = u + wk$ für alle $u \in U$ und alle $w \in W$. (Hier schon haben wir benutzt, dass $\zeta \in Z(\Lambda(U, W))$ gilt.) Ist $\lambda \in \Lambda_1\Lambda_2$, so folgt

$$(u + w)^{\zeta\lambda} = (u + wk)^\lambda = u^\lambda + w^\lambda k = (u^\lambda + w^\lambda)^\zeta = (u + w)^{\lambda\zeta}.$$

Also ist $\zeta\lambda = \lambda\zeta$. Damit ist alles bewiesen.

Mit $C_G(U)$ bezeichnen wir den Zentralisator der Teilmenge U von G in G, dh. die Untergruppe aller mit jedem Element von U vertauschbaren Elemente von G.

5.5. Satz. *Es sei V ein Vektorraum über dem Körper K mit $\mathrm{Rg}_K(V) \geq 3$. Es sei $V = U \oplus W$ mit von $\{0\}$ verschiedenen Unterräumen U und W. Ist dann $1 \neq \lambda \in Z(\Lambda(U,W))$, so gilt*

a) *Gibt es keine Kollineation in $\mathrm{PG^*L}(V)$, die U mit W vertauscht, oder ist $\lambda^2 \neq 1$, so ist*
$$C_{\mathrm{PG^*L}(V)}(\lambda) = \Lambda_1\Lambda_2.$$

b) *Ist $\lambda^2 = 1$ und gibt es eine Kollineation in $\mathrm{PG^*L}(V)$, die U mit W vertauscht, so ist*
$$\left|C_{\mathrm{PG^*L}(V)}(\lambda) : \Lambda_1\Lambda_2\right| = 2,$$
und es gilt $Z(C_{\mathrm{PG^*L}(V)}(\lambda)) = \{1, \lambda\}$.

Beweis. Nach 5.4 f) ist $\Lambda_1\Lambda_2 \subseteq C_{\mathrm{PG^*L}(V)}(\lambda)$. Es sei γ ein Element aus dem Zentralisator von λ. Weil γ die Unterräume, die aus Fixpunkten von λ bestehen, unter sich permutiert, ist $U^\gamma = U$ und $W^\gamma = W$ oder $U^\gamma = W$ und $W^\gamma = U$. Aus 5.4 d) folgt daher, dass $|C_{\mathrm{PG^*L}(V)}(\lambda) : \Lambda_1\Lambda_2| = 1$ oder 2 ist. Es sei nun $\gamma \notin \Lambda_1\Lambda_2$. Dann ist also $U^\gamma = W$ und $W^\gamma = U$. Es sei $(u + w)^\lambda = u + wk$ mit einem geeigneten $k \in Z(K^*)$. Dann gibt es ein $r \in K$ mit
$$w^\gamma + u^\gamma k = (u + w)^{\gamma\lambda} = (u + w)^{\lambda\gamma} r = (u^\gamma + w^\gamma k)r.$$
Hieraus folgt $k = r$ und $kr = 1$. Also ist $k = 1$ oder $k = -1$, so dass a) bewiesen ist.

Ist $\lambda^2 = 1$, so ist $(u + w)^\lambda = u - w$, da ja $\lambda \neq 1$ ist. Ist γ eine Abbildung aus $\mathrm{G^*L}(V)$, die U mit W vertauscht, so ist
$$\begin{aligned}(u + w)^{\lambda\gamma} &= (u - w)^\gamma = u^\gamma - w^\gamma\\ &= -(w^\gamma - u^\gamma) = -(w^\gamma + u^\gamma)^\lambda = -(u + w)^{\gamma\lambda},\end{aligned}$$
woraus folgt, dass $|C_{\mathrm{PG^*L}(V)}(\lambda) : \Lambda_1\Lambda_2| = 2$ ist. Aus a) folgt schließlich noch, dass
$$Z\big(C_{\mathrm{PG^*L}(V)}(\lambda)\big) = \{1, \lambda\}$$
ist, da $Z(K^*)$ nur eine Involution, nämlich -1 enthält.

Sind U und W Unterräume des Vektorraumes V, so bezeichnen wir mit $E(U,W)$ die Menge aller Quasielationen, deren Zentren in U liegen und deren Achsen W enthalten.

Sind X und Y zwei Rechtsvektorräume über dem Körper K, so bezeichnen wir mit $\mathrm{Hom}_K(X,Y)$ die Menge aller linearen Abbildungen von X in Y. Die Menge $\mathrm{Hom}_K(X,Y)$ wird mit der punktweise definierten Addition eine abelsche Gruppe.

5.6. Satz. *Es sei V ein Vektorraum über dem Körper K mit $\mathrm{Rg}_K(V) \geq 3$. Sind U und W Unterräume von V mit $U \leq W$, so ist $\mathrm{E}(U,W)$ eine zu $\mathrm{Hom}_K(V/W,U)$ isomorphe Gruppe.*

Beweis. Setze

$$H := \{\alpha \mid \alpha \in \mathrm{Hom}_K(V,U), W \subseteq \mathrm{Kern}(\alpha)\}.$$

Dann ist H eine Untergruppe von $\mathrm{Hom}_K(V,U)$, die, wie unmittelbar zu sehen, zu $\mathrm{Hom}_K(V/W,U)$ isomorph ist. Ist $\alpha \in H$ und definiert man $\tau(\alpha)$ durch

$$H := \{\alpha \mid \alpha \in \mathrm{Hom}_K(V,U), W \subseteq \mathrm{Kern}(\alpha)\}.$$

Dann ist H eine Untergruppe von $\mathrm{Hom}_K(V,U)$, die wie unmittelbar zu sehen, zu $\mathrm{Hom}_K(V/W,U)$ isomorph ist. Ist $\alpha \in H$ und definiert man $\tau(\alpha)$ durch

$$x^{\tau(\alpha)} := x + x^\alpha$$

für alle $x \in X$ und ist $\tau^*(\alpha)$ die von $\tau(\alpha)$ in $L_K(V)$ induzierte Kollineation, so ist $\tau^*(\alpha) \in \mathrm{E}(U,W)$. Ferner ist τ^* nach dem, was wir bereits wissen, eine Abbildung von H auf $\mathrm{E}(U,W)$.

Sind α, $\beta \in H$, so ist $V^\alpha \leq U \leq W \leq \mathrm{Kern}(\beta)$ und daher $\alpha\beta = 0$. Folglich ist

$$\begin{aligned} x^{\tau(\alpha)\tau(\beta)} &= x + x^\alpha + (x + x^\alpha)^\beta \\ &= x + x^\alpha + x^\beta = x + x^{\alpha+\beta} \\ &= x^{\tau(\alpha+\beta)}. \end{aligned}$$

Dies besagt, dass τ^* ein Homomorphismus von H auf $\mathrm{E}(U,W)$ ist.

Ist $\tau^*(\alpha) = 1$, so gibt es ein $k \in K$ mit $xk = x^{\tau(\alpha)} = x + x^\alpha$ für alle $x \in V$. Nun ist

$$v^\alpha \subseteq U \subseteq W \subseteq \mathrm{Kern}(\alpha).$$

Hieraus folgt, dass α nicht injektiv sein kann, weil das dann $V = \{0\}$ zur Folge hätte. Somit ist der Kern von α nicht trivial. Es gibt also ein $y \in \mathrm{Kern}(\alpha)$ mit $y \neq 0 = y^\alpha$. Dann ist aber $yk = y$ und folglich $k = 1$. Hieraus folgt $x^\alpha = 0$ für alle $x \in V$. Dies zeigt, dass τ^* injektiv ist. Damit ist der Satz bewiesen.

Zur Bestimmung des Zentralisators einer Quasielation benötigen wir noch einige Informationen über die Struktur von Schiefkörpern.

5.7. Satz von Cartan-Brauer-Hua. *Es sei K ein Körper und F sei ein Teilkörper von K. Ist dann $x^{-1}Fx = F$ für alle $x \in K^*$, so ist $F \subseteq Z(K)$ oder $F = K$.*

Beweis. Es sei $k \in K$ und es gebe ein $f \in F$, welches mit k nicht vertauschbar sei. Setze $f_1 := kfk^{-1}$. Dann ist also $f_1 \neq f$, so dass insbesondere $k \neq -1$ ist. Setze $f_2 := (1+k)f(1+k)^{-1}$. Dann ist auch $f_2 \neq f$. Nun ist $(1+k)f = f_2(1+k)$ und folglich $f_2k - kf = f - f_2$. Weiter ist $kf = f_1k$. Also ist

$$0 \neq f - f_2 = f_2k - kf = f_2k - f_1k = (f_2 - f_1)k,$$

so dass $f_2 - f_1 \neq 0$ ist. Daher ist

$$k = (f_2 - f_1)^{-1}(f - f_2).$$

Weil $x^{-1}Fx = F$ für alle $x \in K^*$ gilt, sind $f_1,\ f_2 \in F$. Daher ist $k \in F$. Dies zeigt, dass alle Elemente von K, die F nicht zentralisieren, in F liegen.

Es sei nun $F \not\subseteq Z(K)$. Ist C der Zentralisator von F in K, so ist dann $K - C \neq \emptyset$. Wie wir gerade gesehen haben, gilt $K - C \subseteq F$. Weil $K - C$ nicht leer ist, gibt es ein k in dieser Menge. Dann ist aber $k + C \subseteq K - C$. Folglich gilt $k \in F$. Weil F ein Körper ist, ist dann auch $C \subseteq F$, so dass, wie behauptet, $K = F$ ist.

5.8. Korollar. *Es sei K ein Körper und $k \in K$. Ist $x^{-1}kx$ für alle $x \in K^*$ mit k vertauschbar, so ist $k \in Z(K)$.*

Beweis. Wir dürfen annehmen, dass $k \neq 0$ ist. Es sei C der Zentralisator von k in K und F sei der von allen $x^{-1}kx$ erzeugte Teilkörper. Dieser ist definiert, da k von 0 verschieden ist. Auf Grund unserer Annahme ist $F \subseteq C$. Ferner ist $y^{-1}Fy = F$ für alle $y \in K^*$. Nach dem Satz von Cartan-Brauer-Hua ist daher entweder $F \subseteq Z(K)$ oder $F = K$. Nun ist aber $k = k^{-1}kk \in F$, so dass in beiden Fällen $k \in Z(K)$ gilt, da aus $F = K$ ja $C = K$ folgt.

5.9. Satz. *Es sei K ein Körper der Charakteristik $p > 0$. Ist S eine Untergruppe von K^* und ist Z eine Untergruppe von $Z(K^*)$ mit $Z \subseteq S$, so gilt:*
a) *Ist S/Z eine abelsche p-Gruppe, so ist S abelsch.*
b) *Ist S/Z ein abelscher p-Normalteiler von K^*/Z, so ist $S \subseteq Z(K^*)$.*

Beweis. a) Sind $s,\ t \in S$, so gibt es ein $z \in Z$ mit $t^{-1}st = sz$. Ist p^a die Ordnung von s modulo Z, so ist

$$s^{p^a} = t^{-1}s^{p^a}t = (t^{-1}st)^{p^a} = s^{p^a}z^{p^a},$$

da Z ja im Zentrum von K^* liegt. Also ist $z^{p^a} = 1$. Dies hat $z = 1$ zur Folge, da p ja die Charakteristik von K ist.

b) Ist $k \in K^*$ und $s \in S$, so gibt es ein t in S mit $k^{-1}sk = st$. Ist p^a die Ordnung von s modulo Z, so ist

$$s^{p^a} = k^{-1}s^{p^a}k = (k^{-1}sk)^{p^a} = (st)^{p^a} = s^{p^a}t^{p^a},$$

da ja Z im Zentrum von K liegt. Hieraus folgt wiederum $t^{p^a} = 1$ und damit $t = 1$, so dass $k^{-1}sk = s$ ist. Damit ist alles bewiesen.

Wir nennen *Normalreihe* einer Gruppe eine Kette von Normalteilern dieser Gruppe, wobei sich Kette auf die Inklusion als Teilordnung bezieht. Der Leser beachte, dass die Terminologie in der Literatur nicht einheitlich ist.

5.10. Satz. *Es sei V ein Vektorraum über dem Körper K mit $\mathrm{Rg}_K(V) \geq 3$. Ferner sei τ eine von eins verschiedene Quasielation von $L_K(V)$ mit dem Zentrum U und der Achse W. Setze $H := C_{\mathrm{PG^*L}(V)}(\tau)$. Dann besitzt H eine Normalreihe*

$$\{1\} \subseteq H_2 \subseteq H_1 \subseteq H_0 \subseteq H$$

mit folgenden Eigenschaften:
a) *Ist $\mathrm{Rg}_K(V/W) \geq 2$, so ist $H/H_0 \cong \mathrm{PG^*L}(V/W)$, ist jedoch $\mathrm{Rg}_K(V/W) = 1$, so ist $H/H_0 \cong K^*/Z(K^*)$.*

b) *Es ist* $H_0/H_1 \cong \mathrm{G^*L}(W/U)$.
c) *Es ist* $H_1/H_2 \cong \mathrm{Hom}_K(W/U, U)$.
d) *Es ist* $H_2 \cong \mathrm{Hom}_K(V/W, W)$.
Ferner gilt:
e) $Z(H)$ *ist zur additiven Gruppe von* $Z(K)$ *isomorph.*
f) *Es ist* $Z(H_1) \cong \mathrm{Hom}_K(V/W, U)$.
g) *Ist* $U \neq W$, *so ist* $Z(H_1)$ *echt in* H_2 *enthalten.*
h) *Es ist* $C_H(Z(H_1)) = H_0$.
i) *Ist die Charakteristik* p *von* K *von Null verschieden, so ist* H_1 *der größte auflösbare* p*-Normalteiler von* H.

Beweis. Setze $\alpha := \tau - 1$. Dann ist $U = V^\alpha$ und $W = \mathrm{Kern}(\alpha)$. Dabei haben wir τ mit der linearen Abbildung identifiziert, die τ induziert. Es sei $\gamma \in \mathrm{G^*L}(V)$ und γ induziere in $L_K(V)$ eine Kollineation, die mit der Kollineation τ vertauschbar sei. Es gibt dann ein $k \in K^*$ mit $x^{\tau\gamma} = x^{\gamma\tau}k$ für alle $x \in V$. Hieraus folgt

$$x^\gamma + x^{\alpha\gamma} = x^\gamma k + x^{\gamma\alpha}k$$

für alle $x \in V$. Weil $\tau \neq 1$ ist, ist $U \neq \{0\}$ und daher auch $W \neq \{0\}$. Es gibt also ein von 0 verschiedenes $y \in W$. Wegen $W = \mathrm{Kern}(\alpha)$ ist daher

$$y^\gamma(1 - k) = y^{\gamma\alpha}.$$

Wäre $k \neq 1$, so folgte hieraus

$$y^\gamma \in V^\alpha \subseteq \mathrm{Kern}(\alpha)$$

und damit wiederum $y^\gamma = 0$, was seinerseits den Widerspruch $y = 0$ nach sich zöge. Also ist doch $k = 1$, so dass $\alpha\gamma = \gamma\alpha$ ist. Ist umgekehrt $\gamma \in \mathrm{G^*L}(V)$ und ist γ mit α vertauschbar, so induziert γ ein Element im Zentralisator der Quasielation τ. Somit wird H von $C_{\mathrm{G^*L}(V)}(\alpha)$ induziert, so dass wir zunächst den Zentralisator von α in $\mathrm{G^*L}(V)$ untersuchen. Diesen Zentralisator bezeichnen wir im Folgenden mit C.

Es sei $W = U \oplus S$ und $V = W \oplus T$. Dann ist $V = U \oplus S \oplus T$. Wegen $W = \mathrm{Kern}(\alpha)$ ist $T^\alpha = U$ und wegen $W \cap T = \{0\}$ gibt es zu jedem $u \in U$ genau ein $t \in T$ mit $t^\alpha = u$.

Es sei $\gamma \in C$. Dann ist $U^\gamma = U$. Ist $u \in U$, so ist also

$$u^\gamma = t^{\alpha\gamma} = t^{\gamma_{11}\alpha}$$

mit einem $t \in T$ und einem Endomorphismus γ_{11} von T. Weil die Einschränkung von γ auf U in $\mathrm{G^*L}(U)$ liegt, ist γ_{11} sogar ein Element aus $\mathrm{G^*L}(T)$.

Weil W der Kern von α ist, ist auch $W^\gamma = W$. Ist $s \in S$, so gibt es daher ein $\gamma_{21} \in \mathrm{Hom}_K(S, U)$ und ein $\gamma_{22} \in \mathrm{End}_K(S)$ mit

$$s^\gamma = s^{\gamma_{21}} + s^{\gamma_{22}}.$$

Ist $s^{\gamma_{22}} = 0$, so ist $s^\gamma \in U$. Weil γ bijektiv ist und U invariant lässt, folgt $s \in U$ und damit $s = 0$, da ja $U \cap S = \{0\}$ ist. Dies zeigt, dass γ_{22} injektiv ist. Wegen

$$\begin{aligned} U + S = W = W^\gamma &= U^\gamma + S^\gamma \\ &\subseteq U + S^{\gamma_{21}} + S^{\gamma_{22}} = U + S^{\gamma_{22}} \subseteq U + S \end{aligned}$$

ist $U \oplus S = U + S^{\gamma_{22}}$. Hieraus folgt mittels des Modulargesetzes, dass $S = S^{\gamma_{22}}$ ist. Also ist $\gamma_{22} \in \mathrm{G^*L}(S)$.

Ist schließlich $t \in T$, so gibt es $\gamma_{31} \in \mathrm{Hom}_K(T, U)$, $\gamma_{32} \in \mathrm{Hom}_K(T, S)$ und $\gamma_{33} \in \mathrm{End}_K(T)$ mit

$$t^\gamma = t^{\gamma_{31}} + t^{\gamma_{32}} + t^{\gamma_{33}}.$$

Wegen $U + S = W = \mathrm{Kern}(\alpha)$ folgt

$$t^{\gamma_{11}\alpha} = t^{\alpha\gamma} = t^{\gamma\alpha} = t^{\gamma_{31}\alpha} + t^{\gamma_{32}\alpha} + t^{\gamma_{33}\alpha} = t^{\gamma_{33}\alpha}.$$

Weil die Einschränkung von α auf T injektiv ist, folgt hieraus die Gleichheit von γ_{11} und γ_{33}.

Seien umgekehrt $\gamma_{11} \in \mathrm{G^*L}(T)$ und $\gamma_{22} \in \mathrm{G^*L}(S)$ sowie $\gamma_{21} \in \mathrm{Hom}_K(S, U)$, $\gamma_{31} \in \mathrm{Hom}_K(T, U)$ und $\gamma_{32} \in \mathrm{Hom}_K(T, S)$. Definieren wir γ durch

$$(t^\alpha + s + t_1)^\gamma := t^{\gamma_{11}\alpha} + s^{\gamma_{21}} + s^{\gamma_{22}} + t_1^{\gamma_{31}} + t_1^{\gamma_{32}} + t_1^{\gamma_{11}},$$

so ist $\gamma \in C$, wie wir jetzt zeigen werden.

Weil $t^{\gamma_{11}\alpha} + s^{\gamma_{21}} + s^{\gamma_{22}} + t_1^{\gamma_{31}} + t_1^{\gamma_{32}}$ im Kern von α liegt, ist

$$(t^\alpha + s + t_1)^{\gamma\alpha} = t^{\gamma_{11}\alpha}.$$

Andererseits ist auch $t^\alpha + s$ ein Element des Kerns von α. Daher ist

$$(t^\alpha + s + t_1)^{\alpha\gamma} = t_1^{\alpha\gamma}.$$

Benutzt man schließlich noch einmal die Definition von γ, so folgt $t_1^{\alpha\gamma} = t_1^{\gamma_{11}\alpha}$. Fasst man alles zusammen, so erhält man $\alpha\gamma = \gamma\alpha$.

Wir zeigen, dass γ surjektiv ist. Es ist

$$U^\gamma = T^{\alpha\gamma} = T^{\gamma_{11}\alpha} = T^\alpha = U.$$

Ferner ist

$$s^{\gamma_{22}} = s^\gamma - s^{\gamma_{21}} \in S^\gamma + U$$

und daher $S = S^{\gamma_{22}} \subseteq S^\gamma + U$. Folglich ist

$$W = U + S \subseteq U + S^\gamma = U^\gamma + S^\gamma = W^\gamma,$$

so dass $W = W^\gamma$ ist. Wegen

$$t^{\gamma_{11}} = t^\gamma - t^{\gamma_{31}} - t^{\gamma_{32}} \in T^\gamma + W$$

ist $T = T^{\gamma_{11}} \subseteq T^\gamma + W$ und daher

$$V = W + T \subseteq W + T^\gamma = W^\gamma + T^\gamma = V^\gamma.$$

Dies besagt aber, dass γ surjektiv ist.

Es sei schließlich $0 = (t^\alpha + s + t_1)^\gamma$. Weil V die direkte Summe von U, S und T ist, folgt zunächst $t_1^{\gamma_{11}} = 0$ und damit $t_1 = 0$. Folglich ist

$$t^{\gamma_{11}\alpha} + s^{\gamma_{21}} + s^{\gamma_{22}} = 0.$$

Dies zieht $s^{\gamma_{22}} = 0$ und damit $s = 0$ nach sich. Dann ist aber $t^{\gamma_{11}\alpha} = 0$, was schließlich $t = 0$ impliziert. Also ist γ auch injektiv. Daher gilt das folgende Zwischenresultat:

Ist $\gamma \in C$, so gibt es Abbildungen $\gamma_{11} \in \mathrm{G^*L}(T)$, $\gamma_{22} \in \mathrm{G^*L}(S)$, $\gamma_{21} \in \mathrm{Hom}_K(S,U)$, $\gamma_{31} \in \mathrm{Hom}_K(T,U)$ und $\gamma_{32} \in \mathrm{Hom}_K(T,S)$ mit

$$(t^\alpha + s + t_1)^\gamma = t^{\gamma_{11}\alpha} + s^{\gamma_{21}} + s^{\gamma_{22}} + t_1^{\gamma_{31}} + t_1^{\gamma_{32}} + t_1^{\gamma_{11}};$$

sind umgekehrt γ_{ij} wie gerade beschrieben gegeben und definiert man γ durch diese Gleichung, so ist $\gamma \in C$.

Es sei C_0 diejenige Untergruppe von C, die auf dem Faktorraum V/W die Identität induziert. Es ist $V/W = \{t + W \mid t \in T\}$. Ist $\gamma \in C_0$, so ist also $t^{\gamma_{11}} + W = t + W$ für alle $t \in T$. Wegen $T \cap W = \{0\}$ folgt, dass $\gamma_{11} = 1$ ist. Also gilt $\gamma \in C_0$ genau dann, wenn $\gamma_{11} = 1$ ist. Dies impliziert einmal, dass

$$C/C_0 \cong \mathrm{G^*L}(T) = \mathrm{G^*L}(V/W)$$

ist und dass C_0 auch den Unterraum U vektorweise festlässt.

Es sei C_1 diejenige Untergruppe von C_0, die auf W/U die Identität induziert. Ist $\gamma \in C_1$, so folgt, da $W/U = \{s + U \mid s \in S\}$ ist, dass $s^{\gamma_{22}} + U = s + U$ ist für alle $s \in S$. Weil S und U trivialen Schnitt haben, folgt $\gamma_{22} = 1$. Es ist also genau dann $\gamma \in C_1$, wenn $\gamma_{11} = 1$ und $\gamma_{22} = 1$ ist. Hieraus folgt wiederum

$$C_0/C_1 \cong \mathrm{G^*L}(S) \cong \mathrm{G^*L}(W/U).$$

Es sei C_2 die Untergruppe von C_1, die W vektorweise festlässt. Dann folgt, dass C_1/C_2 zu einer Gruppe von Quasitransvektionen von W isomorph ist, deren Zentren in U liegen und deren Achsen U enthalten. Es sei umgekehrt λ eine Quasitransvektion von W, deren Zentrum in U liegt und deren Achse U enthält. Dann ist also $w^\lambda = w + w^\beta$ mit $\beta \in \mathrm{Hom}_K(W,U)$ und $U \subseteq \mathrm{Kern}(\beta)$. Definiert man nun γ durch

$$(t^\alpha + s + t_1)^\gamma := t^\alpha + s^\beta + s + t_1,$$

so ist $\gamma \in C_1$ und wegen $U \subseteq \mathrm{Kern}(\beta)$ induziert γ in W die Abbildung λ. Nach 5.6 ist folglich

$$C_1/C_2 \cong \mathrm{Hom}_K(W/U, U).$$

Weil die Elemente von C_2 auf W und V/W die Identität induzieren, ist C_2 eine Gruppe von Quasitransvektionen von V, deren Zentren in W enthalten sind und deren Achse W enthalten. Ist umgekehrt μ eine solche Quasitransvektion, so gibt es ein $\mu_{31} \in \mathrm{Hom}_K(T,U)$ und ein $\mu_{32} \in \mathrm{Hom}_K(T,S)$ mit

$$t^\mu = t + t^{\mu_{31}} + t^{\mu_{32}}.$$

Hieraus folgt

$$(t^\alpha + s + t_1)^\mu = t^\alpha + s + t^{\mu_{31}} + t^{\mu_{32}} + t,$$

so dass $\mu \in C_2$ ist. Somit ist

$$C_2 \cong \mathrm{Hom}_K(V/W, W).$$

Wir betrachten nun die von C, C_0, C_1 und C_2 in $L_K(V)$ induzierten Kollineationsgruppen H, H_0, H_1 und H_2. Weil C_i offensichtlich ein Normalteiler von C ist, ist H_i ein Normalteiler von H. Auf Grund des Zwischenresultates ist der Kern des Homomorphismus von C auf H gerade die Gruppe M aller Multiplikationen $\mu(k)$ mit $k \in Z(K^*)$, wobei $\mu(k)$, wie schon zuvor, durch $v^{\mu(k)} := vk$ definiert ist. Es folgt, dass MC_i das Urbild von H_i in C ist. Ferner ist $M \cap C_i = \{1\}$, da U wegen $\tau \neq 1$ mindestens den Rang 1 hat und U von C_i vektorweise festgelassen wird. Setzt man noch $C_3 := \{1\}$ und $H_3 := \{1\}$, so folgt für $i := 0$, 1, 2, dass

$$\begin{aligned} H_i/H_{i+1} &\cong (MC_i)/(MC_{i+1}) = (MC_{i+1}C_i)/(MC_{i+1}) \\ &\cong C_i/(C_i \cap MC_{i+1}) = C_i/C_{i+1} \end{aligned}$$

ist, da ja wegen $C_{i+1} \subseteq C_i$ auf Grund des Modulargesetzes die Gleichungen

$$C_i \cap MC_{i+1} = (C_i \cap M)C_{i+1} = C_{i+1}$$

gelten. Damit ist die Gültigkeit von b), c) und d) bewiesen.

Betrachtet man die Abbildungen $\gamma \in C$ mit $\gamma_{21} = 0$, $\gamma_{31} = 0$, $\gamma_{32} = 0$ und $\gamma_{22} = 1$, so bilden diese eine Untergruppe D von C. Es ist $C = DC_0$ und $D \cap C_0 = \{1\}$. Ferner sieht man sofort, dass $D \cap MC_0 = Z(D)$ ist. Daher ist

$$H/H_0 \cong C/(MC_0) = (DMC_0)/(MC_0) \cong D/(D \cap MC_0) = D/Z(D),$$

so dass auch a) gilt.

Als Nächstes bestimmen wir $Z(H)$. Es sei $\delta M \in Z(H)$. Ist $\gamma \in C$, so gibt es wegen $\mathrm{Rg}_K(V) \geq 3$ nach 1.2 ein $k_\gamma \in Z(K^*)$ mit $v^{\gamma\delta} = v^{\delta\gamma}k_\gamma$ für alle $v \in V$. Insbesondere ist dann

$$t^{\gamma_{11}\delta_{11}\alpha} = t^{\gamma_{11}\alpha\delta} = t^{\alpha\gamma\delta} = t^{\alpha\delta\gamma}k_\gamma = t^{\delta_{11}\gamma_{11}\alpha}k_\gamma = (t^{\delta_{11}\gamma_{11}}k_\gamma)^\alpha$$

und daher

$$t^{\gamma_{11}\delta_{11}} = t^{\delta_{11}\gamma_{11}}k_\gamma$$

für alle $t \in T$. Weil γ_{11} alle Werte in $\mathrm{G^*L}(T)$ annimmt und das Zentrum der Gruppe $\mathrm{PG^*L}(T)$ trivial ist, folgt, dass δ_{11} alle Punkte von $L_K(T)$ festlässt.

Ist $\mathrm{Rg}_K(T) \leq 2$, so gibt es nach 1.2 ein $k \in Z(K^*)$ mit $t^{\delta_{11}} = tk$ für alle $t \in T$. Es sei $\mathrm{Rg}_K(T) = 1$ und $T = t_0K$. Es gibt dann ein $k \in K^*$ mit $t_0^{\delta_1} = t_0k$. Ist nun $m \in K^*$, so gibt es ein $\gamma_{11} \in \mathrm{G^*L}(T)$ mit $t_0^{\gamma_{11}} = t_0m$. Es gibt ferner ein $\gamma \in C$, welches dieses γ_{11} induziert. Damit folgt

$$t_0km = t_0^{\delta_{11}}m = t_0^{\gamma_{11}\delta_{11}} = t_0^{\delta_{11}\gamma_{11}}k_\gamma = t_0^{\gamma_{11}}k_\gamma = t_0mkk_\gamma.$$

Hieraus folgt die Gleichung $km = mkk_\gamma$. Weil k_γ im Zentrum von K liegt ist daher

$$km^{-1}km = k^2k_\gamma = kk_\gamma k = m^{-1}kmk.$$

Weil dies für alle von Null verschiedenen m aus K gilt, folgt mit 5.8, dass $k \in Z(K^*)$ ist. Es gilt also in jedem Falle, dass $t_{11}^{\delta} = tk$ für alle $t \in T$ gilt, wobei k ein passendes Elemente aus dem Zentrum von K ist. Hiermit folgt weiter

$$t^{\gamma_{11}}k = t^{\gamma_{11}\delta_{11}} = t^{\delta_{11}\gamma_{11}}k_\gamma = t^{\gamma_{11}}kk_\gamma$$

und dann $k = kk_\gamma$, so dass $k_\gamma = 1$ ist. Da dies für alle $\gamma \in C$ gilt, liegt δ im Zentrum von C, so dass also $Z(C)$ das Urbild von $Z(H)$ ist.

Weil k im Zentrum von K liegt, folgt, dass die durch $v^\eta := v^\delta k^{-1}$ erklärte Abbildung η in C und damit in C_0 liegt. Da η und δ die gleiche Kollineation in $L_K(V)$ induzieren, folgt, dass $Z(C) \cap C_0$ bei dem Homomorphismus von C auf H auf $Z(H)$ abgebildet wird. Weil die Einschränkung dieses Homomorphismus auf C_0 wegen $M \cap C_0 = \{1\}$ ein Monomorphismus ist, sind $Z(C) \cap C_0$ und $Z(H)$ isomorph.

Es sei $\gamma \in C$ und $\delta \in Z(C) \cap C_0$. Wegen $\delta_{11} = 1$ ist dann

$$s^{\gamma\delta} = (s^{\gamma_{21}} + s^{\gamma_{22}})^\delta = s^{\gamma_{21}} + s^{\gamma_{22}\delta_{21}} + s^{\gamma_{22}\delta_{22}}.$$

Andererseits ist

$$s^{\delta\gamma} = (s^{\delta_{21}} + s^{\delta_{22}})^\gamma = s^{\delta_{21}\gamma} + s^{\delta_{22}\gamma_{21}} + s^{\delta_{22}\gamma_{22}}.$$

Wegen $\gamma\delta = \delta\gamma$ folgen die Gleichungen

$$s^{\gamma_{21}} + s^{\gamma_{22}\delta_{21}} = s^{\delta_{21}\gamma} + s^{\delta_{22}\gamma_{21}}$$

und

$$s^{\gamma_{22}\delta_{22}} = s^{\delta_{22}\gamma_{22}}.$$

Da γ_{22} aller Werte in $\mathrm{G^*L}(S)$ fähig ist, folgt wieder die Existenz eines $k \in Z(K^*)$ mit $s^{\delta_{22}} = sk$ für alle $s \in S$. Hieraus folgt mittels der ersten Gleichung

$$s^{\gamma_{21}}(1-k) = s^{\delta_{21}\gamma} - s^{\gamma_{22}\delta_{21}}.$$

Mit Hilfe des Zwischenresultates folgt, dass γ_{21} auch dann noch aller Werte in $\mathrm{Hom}_K(S, U)$ fähig ist, wenn γ auf U die Identität induziert und $\gamma_{22} = 1$ ist. Daher gilt

$$s^{\gamma_{21}}(1-k) = 0$$

für alle $s \in S$ und alle $\gamma_{21} \in \mathrm{Hom}_K(S, U)$. Ist $S \neq \{0\}$, so folgt $k = 1$. Daher ist in jedem Falle $\delta_{22} = 1$ und

$$0 = s^{\delta_{21}\gamma} - s^{\gamma_{22}\delta_{21}}.$$

Hieraus folgt weiter, wiederum auf Grund des Zwischenresultates, dass $\delta_{21} = 0$ ist, es sei denn, es ist $K = \mathrm{GF}(2)$ und $\mathrm{Rg}_K(U) = \mathrm{Rg}_K(S) = 1$ und folglich $\mathrm{Rg}_K(V) = 3$. Dieser Fall kann aber nicht eintreten, wie wir gleich sehen werden.

Nun ist einerseits

$$t^{\gamma\delta} = t^{\gamma_{31}} + t^{\gamma_{32}\delta_{21}} + t^{\gamma_{32}} + t^{\gamma_{11}\delta_{3}1} + t^{\gamma_{11}\delta_{32}} + t^{\gamma 11}$$

und andererseits

$$t^{\delta\gamma} = t^{\delta_{31}\gamma} + t^{\delta_{32}\gamma_{21}} + t^{\delta_{32}\gamma_{22}} + t^{\gamma_{31}} + t^{\gamma_{32}} + t^{\gamma_{11}}.$$

Wegen $\gamma\delta = \delta\gamma$ folgen die beiden Gleichungen

$$t^{\gamma_{32}\delta_{21}} + t^{\gamma_{11}\delta_{31}} = t^{\delta_{31}\gamma} + t^{\delta_{31}\gamma_{21}}$$

und

$$t^{\gamma_{11}\delta_{32}} = t^{\delta_{32}\gamma_{22}}.$$

Wäre $\delta_{21} \neq 0$, so wäre also $\mathrm{Rg}_K(U) = \mathrm{Rg}_K(S) = \mathrm{Rg}_K(T) = 1$ und $K = \mathrm{GF}(2)$. Daher wäre $\gamma_{11} = 1$ und $\gamma_{22} = 1$ und folglich $t^{\gamma_{32}\delta_{21}} = t^{\delta_{32}\gamma_{21}}$, da ja dann $t^{\delta_{31}\gamma} = t^{\delta_{31}}$ ist. Mit $\gamma_{21} = 0$ und $\gamma_{32} \neq 0$ folgte der Widerspruch $\delta_{21} = 0$. Also ist in jedem Falle $\delta_{21} = 0$.

Wäre $\delta_{32} \neq 0$, so folgte wiederum, dass $K = \mathrm{GF}(2)$ und

$$\mathrm{Rg}_K(U) = \mathrm{Rg}_K(S) = \mathrm{Rg}_K(T) = 1$$

wäre. Dann wäre $\gamma_{11} = 1$ und folglich

$$t^{\delta_{31}} = t^{\delta_{31}} + t^{\delta_{32}\gamma_{21}},$$

woraus $\gamma_{21} = 0$ folgte. Das zöge aber den Widerspruch

$$\{0\} = \mathrm{Hom}_K(S, U) \neq \{0\}$$

nach sich. Also ist doch $\delta_{32} = 0$.

Damit ist gezeigt: Ist $\delta \in Z(C) \cap C_0$, so ist

$$(t^\alpha + s + t_1)^\delta = t^\alpha + s + t_1^{\delta_{31}} + t_1,$$

wobei δ_{31} der Bedingung $\gamma_{11}\delta_{31} = \delta_{31}\gamma$ für alle $\gamma \in C$ genügt. Umgekehrt sieht man unmittelbar, dass auch jede solche Abbildung δ in $Z(C) \cap C_0$ liegt.

Ist $1 \neq \delta \in Z(C) \cap C_0$, so ist $\delta_{31} \neq 0$. Bezeichnet man mit β die Einschränkung von α auf T, so ist β ein Isomorphismus von T auf U. Es folgt, dass auch $\delta_{31}\beta^{-1} \neq 0$ ist. Ferner ist

$$\gamma_{11}\delta_{31} = \delta_{31}\gamma = \delta_{31}\beta^{-1}\alpha\gamma = \delta_{31}\beta^{-1}\gamma_{11}\alpha,$$

so dass also

$$\gamma_{11}\delta_{31}\beta^{-1} = \delta_{31}\beta^{-1}\gamma_{11}$$

ist. Hieraus folgt, dass $\delta_{31}\beta^{-1} \in Z(\mathrm{G^*L}(T))$ ist. Dies impliziert, auch im Falle $\mathrm{Rg}_K(T) = 1$, dass es ein $k \in Z(K^*)$ gibt mit

$$t^{\delta_{31}\beta^{-1}} = tk$$

dh. mit

$$t^{\delta_{31}} = t^\alpha k$$

für alle $t \in T$. Damit ist gezeigt, dass

$$(t^\alpha + s + t_1)^\delta = t^\alpha + s + t_1^\alpha k + t_1$$

ist.

Ist umgekehrt $k \in Z(K^*)$ und definiert man δ durch die gerade etablierte Gleichung, so liegt δ in $Z(C) \cap C_0$. Hieraus folgt die Behauptung unter e).

Es seien γ, $\delta \in C_1$ und es gelte $\delta M \in Z(H_1)$. Es gibt dann ein $k \in Z(K^*)$ mit $v^{\gamma\delta} = v^{\delta\gamma}k$. Hieraus folgt wegen $\gamma_{11} = \delta_{11} = 1$, dass

$$t^{\alpha\gamma\delta} = t^{\alpha\delta\gamma}k$$

ist. Dies hat $k = 1$ zur Folge. Hieraus folgt weiter, dass $Z(H_1)$ von $Z(C_1)$ induziert wird.

Es sei $\gamma \in C_1$ und $\delta \in Z(C_1)$. Dann ist

$$t^{\gamma\delta} = t^{\gamma_{31}} + t^{\gamma_{32}\delta_{21}} + t^{\gamma_{32}} + t^{\delta_{31}} + t^{\delta_{32}} + t$$

und

$$t^{\delta\gamma} = t^{\delta_{31}} + t^{\delta_{32}\gamma_{21}} + t^{\delta_{32}} + t^{\gamma_{31}} + t^{\gamma_{32}} + t.$$

Somit ist $\gamma_{32}\delta_{21} = \delta_{32}\gamma_{21}$ für alle γ_{21}. Hieraus folgt $\delta_{21} = 0$ und $\delta_{32} = 0$. Nun sind die Elemente aus C_2 gerade die Elemente η mit $\eta_{11} = 1$, $\eta_{21} = 0$. Ist nun $U \neq W$, so gibt es ein $\eta \in C_2$ mit $\eta_{32} \neq 0$, so dass in diesem Falle $Z(C_1)$ echt in C_2 enthalten ist. Hieraus folgt die Gültigkeit von g).

Es sei $\delta \in C_2$. Dann ist $\delta_{11} = 1$, $\delta_{22} = 1$ und $\delta_{21} = 0$. Ist auch noch $\delta_{32} = 0$, so überzeugt man sich leicht, dass $\delta \in Z(C_1)$ ist. Dies impliziert f).

Es sei $\gamma \in C$ und $v^{\gamma\delta} = v^{\delta\gamma}k_\delta$ für alle $\delta \in Z(C_1)$, wobei k_δ ein von δ abhängiges Element aus $Z(K^*)$ sei. Ist $u \in U$, so ist auch $u^\gamma \in U$. Daher ist $u^\delta = u$ und $u^{\gamma\delta} = u^\gamma$. Also ist

$$u^\gamma = u^{\gamma\delta} = u^{\delta\gamma}k_\delta = u^\gamma k_\delta,$$

so dass $k_\delta = 1$ ist, da ja $U \neq \{0\}$ ist. Somit sind γ und δ miteinander vertauschbar.

Es ist

$$t^{\gamma\delta} = t^{\gamma_{31}} + t^{\gamma_{32}} + t^{\gamma_{11}\delta_{31}} + t^{\gamma_{11}}$$

und

$$t^{\delta\gamma} = t^{\delta_{31}\gamma} + t^{\gamma_{31}} + t^{\gamma_{32}} + t^{\gamma_{11}}.$$

Also ist $\gamma_{11}\delta_{31} = \delta_{31}\gamma$ für alle $\delta_{31} \in \mathrm{Hom}_K(T, U)$. Dies impliziert, wie schon mindestens zweimal gesehen, dass $t^{\gamma_{11}} = tz$ ist mit einem $z \in Z(K^*)$. Nun induzieren γ und die durch $v^\eta := v^\gamma z^{-1}$ definierte Abbildung η die gleiche Kollineation in $L_K(V)$. Daher ist $C_H(Z(H_1)) \subseteq H_0$. Eine triviale Rechnung zeigt schließlich, dass $C_H(Z(H_1)) = H_0$ ist.

Aus c) und d) folgt, dass $H_1^{(2)} = \{1\}$ ist. Daher ist H_1 auflösbar. Ist $p := \mathrm{Char}(K) > 0$, so folgt ebenfalls aus c) und d), dass $\eta^{p^2} = 1$ ist für alle $\eta \in H_1$. Somit ist H_1 ein auflösbarer p-Normalteiler von H. Es sei G

ein auflösbarer p-Normalteiler von H. Dann ist auch GH_1 ein auflösbarer p-Normalteiler, so dass wir annehmen dürfen, dass $H_1 \subseteq G$ ist.

Ist $G \cap H_0 \neq H_1$, so ist $(G \cap H_0)/H_1$ ein nicht trivialer p-Normalteiler von H_0/H_1. Aus b) folgt dann, dass $\mathrm{G^*L}(W/U)$ einen nicht trivialen p-Normalteiler N enthält. Hieraus folgt $\mathrm{Rg}_K(W/U) \leq 2$, denn andernfalls enthielte K^* einen nicht trivialen p-Normalteiler, was wegen $\mathrm{Char}(K) = p > 0$ nicht der Fall ist. Nun ist $Z(\mathrm{G^*L}(W/U))$ zu $Z(K^*)$ isomorph, so dass auch das Zentrum von $\mathrm{G^*L}(W/U)$ keinen nicht trivialen p-Normalteiler enthält. Weil $\mathrm{SL}(W/U)$ keine p-Gruppe ist, folgt $\mathrm{SL}(W/U) \not\subseteq N$. Nach 2.9 ist daher W/U der Vektorraum vom Range 2 über $\mathrm{GF}(2)$ oder $GF(3)$. Dies kann aber nicht sein, da $\mathrm{GL}(2,2)$ keinen nicht trivialen 2-Normalteiler und $\mathrm{GL}(2,3)$ keinen nicht trivialen 3-Normalteiler besitzt. Also ist $G \cap H_0 = H_1$.

Es sei $G \neq H_1$. Wegen $G \cap H_0 = H_1$ ist dann $(GH_0)/H_0$ ein nicht trivialer p-Normalteiler von H/H_0. Wäre $\mathrm{Rg}_K(V/W) \geq 2$, so hätte $\mathrm{PG^*L}(V/W)$ einen nicht trivialen p-Normalteiler, was mit Hilfe von 2.8 auf einen Widerspruch führte. Also ist $\mathrm{Rg}_K(V/W) = 1$ und es folgt, dass $K^*/Z(K^*)$ einen nicht trivialen, auflösbaren p-Normalteiler $N/Z(K^*)$ hat. Es gibt eine natürliche Zahl i mit $N^{(i)} \not\subseteq Z(K^*)$ und $N^{(i+1)} \subseteq Z(K^*)$. Weil $N^{(i)}$ in N charakteristisch ist, ist $N^{(i)}$ ein Normalteiler von $K^*/Z(K^*)$ ist. Nach 5.9 b) ist daher $N^{(i)} \subseteq Z(K^*)$. Dieser Widerspruch zeigt, dass $G = H_1$ ist, so dass 5.10 vollständig bewiesen ist.

Wir schließen diesen Abschnitt mit einem Korollar zu Satz 5.10, das zu beweisen dem Leser als Übungsaufgabe überlassen sei.

5.11. Korollar. *Ist V ein Vektorraum über dem Körper K mit $\mathrm{Rg}_K(V) \geq 3$, so sind die folgenden Aussagen äquivalent:*

a) *$L_K(V)$ ist pappossch.*

b) *Ist (OP, H) ein inzidentes Punkt-Hyperebenenpaar von $L_K(V)$ und sind σ, τ zwei von eins verschiedene Elationen aus $\mathrm{E}(P,H)$, so ist $C_{\mathrm{PG^*L}(V)}(\sigma) = C_{\mathrm{PG^*L}(V)}(\tau)$.*

c) *Es gibt ein inzidentes Punk-Hyperebenenpaar (P,H) von $L_K(V)$, so dass für alle von eins verschiedenen Elationen σ und τ aus $\mathrm{E}(P,H)$ gilt, dass $C_{\mathrm{PG^*L}(V)}(\sigma) = C_{\mathrm{PG^*L}(V)}(\tau)$ ist.*

6. Zentralisatoren von Involutionen

Involutorische Streckungen und involutorische Elationen lassen sich an Hand ihrer Zentralisatoren von anderen involutorischen Kollineationen unterscheiden. Dies zu zeigen ist Ziel dieses Abschnitts. Im nächsten Abschnitt machen wir dann davon Gebrauch und zeigen, dass die projektive Geometrie $L_K(V)$ durch die Gruppe $\mathrm{PG^*L}(V)$ bis auf Isomorphie oder Antiisomorphie festgelegt ist.

6.1. Satz. *Es sei V ein Vektorraum über dem Körper K mit $\mathrm{Rg}_K(V) \geq 1$. Ferner sei α ein innerer Automorphismus von K. Ist dann $\sigma \in \Gamma\mathrm{L}(V)$ eine semilineare Abbildung mit begleitendem Automorphismus α, ist $\gamma \in \mathrm{G^*L}(V)$, sind k, $m \in K$ und gilt $v^{\sigma^2} = vk$ sowie $v^{\sigma\gamma} = v^{\gamma\sigma}m$ für alle $v \in V$, so ist $m = 1$ oder $m = -1$.*

Beweis. Es ist

$$v^{\gamma\sigma}mx^{\alpha} = v^{\sigma\gamma}x^{\alpha} = (vx)^{\sigma\gamma} = (vx)^{\gamma\sigma}m = v^{\gamma\sigma}x^{\alpha}m.$$

Also ist $mx^{\alpha} = x^{\alpha}m$ für alle $x \in K$. Somit liegt m im Zentrum von K. Weil α ein innerer Automorphismus von K ist, ist daher $m^{\alpha} = m$. Hiermit folgt, dass

$$v^{\gamma}k = v^{\gamma\sigma^2} = (v^{\sigma\gamma}m^{-1})^{\sigma} = v^{\sigma\gamma\sigma}m^{-1} = v^{\sigma^2\gamma}m^{-2} = v^{\gamma}km^{-2}$$

ist. Somit ist $k = km^{-2}$, woraus $m^2 = 1$ und damit die Behauptung folgt, da m ja im Zentrum liegt.

6.2. Satz. *Es sei V ein Vektorraum über dem Körper K mit $\mathrm{Rg}_K(V) \geq 3$. Es sei σ eine Involution aus $\mathrm{PG^*L}(V)$, die in $L_K(V)$ keinen Fixpunkt habe, und C sei der Zentralisator von σ in $\mathrm{PG^*L}(V,K)$. Mit ρ bezeichnen wir eine lineare Abbildung, die σ induziert, und mit F den Teilring von $\mathrm{End}_Z(V)$, der von K und ρ erzeugt wird. Dann gilt:*
a) *F ist ein Körper und quadratische Erweiterung von K.*
b) *V ist auch ein Vektorraum über F.*
c) *Ist $\mathrm{Char}(K) = 2$, so ist $C/Z(C) \cong \mathrm{PG^*L}(V,F)$ und $Z(C) \cong Z(F^*)/Z(K^*)$.*
d) *Ist $\mathrm{Char}(K) \neq 2$, so besitzt C einen Normalteiler N vom Index 2 mit $N/Z(N) \cong \mathrm{PG^*L}(V,F)$ und $Z(N) \cong Z(F^*)/Z(K^*)$. Ferner ist $Z(C) = \{1,\sigma\}$.*

Beweis. Weil σ eine Involution ist, gibt es ein $k \in Z(K^*)$ mit $v^{\rho^2} = vk$ für alle $v \in V$. Weil ρ eine lineare Abbildung ist und k im Zentrum von k liegt, ist

$$F = \{a + b\rho \mid a, b \in K\}.$$

Es sei $0 \neq v \in V$. Dann ist vF ein Teilmodul des F-Moduls V und es ist $vF = vK + v^{\rho}K$. Weil σ keinen Fixpunkt hat, ist $v^{\rho} \notin vK$. Daher ist sogar $vF = vK \oplus v^{\rho}K$. Dies impliziert, dass aus $0 = v(a + b\rho) = va + v^{\rho}b$ folgt, dass $a = b = 0$ ist.

Es sei R ein von $\{0\}$ verschiedenes Rechtsideal von F. Dann ist nach dem gerade Bewiesenen vR ein von Null verschiedener F-Teilmodul von vF. Weil K in F enthalten ist, ist vF auch ein Teilraum des K-Vektorraumes V. Weil σ keinen Fixpunkt hat, folgt aus $vR \neq \{0\}$, dass der Rang von vR als K-Vektorraum mindestens 2 ist. Da andererseits $\mathrm{Rg}_K(vF) = 2$ ist, ist $vR = vF$. Es sei nun $f \in F$. Es gibt dann ein $r \in R$ mit $vr = vf$. Hieraus folgt $v(r-f) = 0$. Dies hat $r - f = 0$ zur Folge, wie wir oben gesehen haben. Also ist $F = R$, so dass F das einzige von Null verschiedene Rechtsideal von F ist. Dies impliziert, dass F ein Körper ist. Damit sind a) und b) bewiesen.

Es sei α die durch $(a + b\rho)^{\alpha} := a - b\rho$ definierte Abbildung. Triviale Rechnungen zeigen, dass α ein Automorphismus von F ist. Ist die Charakteristik von K gleich 2, so ist $\alpha = 1$. Ist die Charakteristik von K von 2 verschieden, so ist α involutorisch. Ist nun γ ein Element aus $\mathrm{G^*L}(V,K)$, welches eine Kollineation aus C in $L_K(V)$ hervorruft, so ist nach 6.1 entweder $\rho\gamma = \gamma\rho$ oder $\rho\gamma = -\gamma\rho$. Im ersten Falle ist $(v(a + b\rho))^{\gamma} = v^{\gamma}(a + b\rho)$, dh., es ist $\gamma \in \mathrm{G^*L}(V,F)$, und im

zweiten Falle ist $(v(a+b\rho))^\gamma = v^\gamma(a+b\rho)^\alpha$, dh., γ ist eine semilineare Abbildung des F-Vektorraumes V mit begleitendem Automorphismus α. Umgekehrt sieht man, dass jedes Element aus $\mathrm{G^*L}(V,F)$ und jede bijektive semilineare Abbildung des F-Vektorraumes V mit α als begleitendem Automorphismus eine Kollineation in $L_K(V)$ induziert, die in C liegt. Aus diesem Bemerkungen folgen die Aussagen c) und d) bis auf die Aussage über das Zentrum von C unter d).

Es ist klar, dass $Z(C) \subseteq Z(N)$ ist. Es sei also $f \in Z(F^*)$ und γ sei eine bezüglich α semilineare Abbildung des F-Vektorraumes V. Ferner induziere die durch $v^\zeta := vf$ definierte Abbildung ζ eine Kollineation aus $Z(C)$. Dann gibt es ein $k \in K^*$ mit

$$vfk = v^\zeta k = v^{\gamma^{-1}\zeta\gamma} = (v^{\gamma^{-1}}f)^\gamma = vf^\alpha.$$

Also ist $fk = f^\alpha$. Weil K von α elementweise festgelassen wird und weil $\alpha^2 = 1$ ist, ist also $k^2 = 1$ und damit $k = 1$ oder $k = -1$. Im ersten Fall folgt $f \in K$, so dass ζ die Identität induziert. Im zweiten Falle folgt $v^\zeta = v^\rho b$ mit einem $b \in K^*$, so dass ζ die Abbildung ρ induziert. Damit ist 6.2 bewiesen.

Eine Bemerkung ist angebracht. Hat im vorliegenden Falle V endlichen Rang, so ist $\mathrm{Rg}_K(V) = 2 \cdot \mathrm{Rg}_F(V)$, so dass $\mathrm{Rg}_K(V)$ gerade ist.

6.3. Satz. *Es sei K ein Körper und α sei ein involutorischer Automorphismus von K. Ist dann $F := \{f \mid f \in K, f^\alpha = f\}$ der Fixkörper von α, so gilt:*

a) *Ist* $\mathrm{Char}(K) \neq 2$, *so gibt es ein $j \in K$ mit $j^\alpha = -j \neq 0$. Ist $j^\alpha = -j \neq 0$, so ist $K = F \oplus jF$.*

b) *Ist* $\mathrm{Char}(K) = 2$, *so gibt es ein $j \in K$ mit $j^\alpha = j+1$. Ist $j^\alpha = j+1$, so ist $K = f \oplus jF$.*

In beiden Fällen ist $[K : F] = 2$.

Beweis. a) Weil $\alpha \neq 1$ ist, gibt es ein $x \in K$ mit $x^\alpha \neq x$. Setze $j := x - x^\alpha$. Dann ist $j^\alpha = -j \neq 0$.

Es sei $j^\alpha = -j \neq 0$. Dann ist $F \cap jF = \{0\}$. Ist $k \in K$, so ist

$$k = \frac{1}{2}(k + k^\alpha) + \frac{1}{2}(k - k^\alpha).$$

Ferner ist $\frac{1}{2}(k+k^\alpha) \in F$. Weil j von 0 verschieden ist, gibt es ein $r \in K$ mit $\frac{1}{2}(k-k^\alpha) = jr$. Dann ist

$$-jr = \frac{1}{2}(k - k^\alpha) = \left(\frac{1}{2}\big(k - k^\alpha\big)\right)^\alpha = (jr)^\alpha = -jr^\alpha,$$

so dass $r^\alpha = r$ ist. Folglich ist $r \in F$, so dass $K = F + jF$ ist. Also ist $K = F \oplus jF$.

b) Es sei $x^\alpha \neq x$ und $r(x^\alpha + x) = 1$ Wegen $x^\alpha + x \in F$ ist dann auch $r \in F$. Setze $j := rx$. Dann ist

$$j^\alpha + j = (rx)^\alpha + rx = r(x^\alpha + x) = 1$$

und folglich, da die Charakteristik ja 2 ist, $j^\alpha = j + 1$.

Es sei nun $j^\alpha = j + 1$. Wegen $j \neq j + 1$ ist $j^\alpha \neq j$ und daher $F \cap jF = \{0\}$. Ist $k \in K$, so ist $k + k^\alpha \in F$. Ferner ist

$$\bigl(k + j(k + k^\alpha)\bigr)^\alpha = k^\alpha + (j + 1)(k + k^\alpha) = k + j(k + k^\alpha).$$

Also ist auch $k + j(k + k^\alpha) \in F$. Schließlich ist

$$k = k + j(k + k^\alpha) + j(k + k^\alpha) \in F + jF.$$

Damit ist alles bewiesen.

Als Nächstes beweisen wir einen Spezialfall von Hilberts Satz 90.

6.4. Satz. *Es sei K ein Körper und α sei ein involutorischer Automorphismus von K. Ist $a \in K$, so sind die folgenden Aussagen äquivalent:*
a) *Es ist $aa^\alpha = 1$.*
b) *Es gibt ein $b \in K$ mit $a = b^\alpha b^{-1}$.*
c) *Es gibt ein $c \in K$ mit $a = cc^{-\alpha}$.*

Beweis. a) impliziert b). Es sei $aa^\alpha = 1$. Wäre $x + a^{-1}x^\alpha = 0$ für alle $x \in K$, so folgte mit $x = 1$, dass $a^{-1} = -1$ wäre. Es folgte der Widerspruch $x^\alpha = x$ für alle $x \in K$. Es gibt folglich ein $x \in K$, so dass $x + a^{-1}x^\alpha \neq 0$ ist. Setze $b := x + a^{-1}x^\alpha$. Dann ist

$$b^\alpha b^{-1} = (x^\alpha + a^{-\alpha}x)b^{-1} = (x^\alpha + ax)b^{-1} = abb^{-1} = a.$$

b) impliziert c). Es sei $a = b^\alpha b^{-1}$. Setze $c := b^\alpha$. Dann ist $c \neq 0$ und $a = cc^{-\alpha}$.

c) impliziert a). Ist nämlich $a = cc^{-\alpha}$, so ist $aa^\alpha = cc^{-\alpha}c^\alpha c^{-1} = 1$. Damit ist alles bewiesen.

6.5. Satz. *Es sei V ein Vektorraum über dem Körper K mit $\mathrm{Rg}_K(V) \geq 3$. Ferner sei σ eine Involution aus $\mathrm{PG^*L}(V, K)$, die einen Fixpunkt besitzt.*

Wird σ nicht durch eine Involution aus $\mathrm{G^*L}(V, K)$ induziert, so gibt es einen inneren Automorphismus α der Ordnung 2 von K und eine bezüglich α semilineare Abbildung η von V in sich mit $\eta^2 = 1$, welche σ induziert.

Ist F der Fixkörper von α und ist W die Menge der Fixvektoren von η, so ist V auch ein F-Vektorraum und W ist ein Teilraum des F-Vektorraumes V. Ferner gilt $\mathrm{Rg}_V(W) = \mathrm{Rg}_K(V)$.

Ist C der Zentralisator von σ in $\mathrm{PG^*L}(V, K)$, so gilt:
a) *Ist $\mathrm{Char}(K) = 2$, so ist*

$$C/Z(C) \cong \mathrm{PG^*L}(W, F) \quad \textit{und} \quad Z(C) \cong Z(F^*)/Z(K^*).$$

b) *Ist $\mathrm{Char}(K) \neq 2$, so enthält C einen Normalteiler N vom Index 2 und es ist*

$$N/Z(N) \cong \mathrm{PG^*L}(W, F) \quad \textit{sowie} \quad Z(N) \cong Z(F^*)/Z(K^*).$$

Ferner ist $Z(C) = \{1, \sigma\}$.

Beweis. Es sei $\rho \in \mathrm{G^*L}(V,K)$ und ρ induziere σ. Ferner sei $P = pK$ ein nach Voraussetzung existierender Fixpunkt von σ. Es gibt dann ein $k \in K^*$ mit $p^\rho = pk$ und ein $z \in Z(K^*)$ mit $v^{\rho^2} = vz$ für alle $v \in V$. Hieraus folgt, dass $k^2 = z \in Z(K)$ ist. Definiert man α durch $x^\alpha := kxk^{-1}$ für alle $x \in K$, so ist α ein innerer Automorphismus von K mit $\alpha^2 = 1$.

Es sei η die durch $v^\eta := v^\rho k^{-1}$ definierte semilineare Abbildung von V in sich. Dann wird σ auch von η induziert. Ferner ist $v^{\eta^2} = v^{\rho^2} k^{-2} = v$, so dass $\eta^2 = 1$ ist. Weil σ von η induziert wird, folgt auf Grund unserer Annahme, dass η nicht linear ist. Folglich ist $k \notin Z(K)$ und daher $\alpha \neq 1$. Ist $x \in K$, so ist

$$(vx)^\eta = (vx)^\rho k^{-1} = v^\rho x k^{-1} = v^\eta x^\alpha,$$

so dass α der begleitende Automorphismus von η ist.

Die Existenz von η und α etabliert, sei F der Fixkörper von α. Dann ist V auch ein Vektorraum über F und es gilt $\eta \in \mathrm{G^*L}(V,F)$. Wie im Satz notiert, sei W die Menge der Fixvektoren von η. Dann ist W ein Teilraum des F-Vektorraumes V.

1) Ist M eine Menge von linear unabhängigen Vektoren des F-Vektorraumes W, so ist M eine linear unabhängige Teilmenge des K-Vektorraumes V.

Es seien $m_1, \ldots, m_n \in M$ und $x_1, \ldots, x_n \in K$ und es gelte $\sum_{i:=1}^n m_i x_i = 0$. Dann ist auch $\sum_{i:=1}^n m_i x_i y = 0$ für alle $y \in K$. Hieraus folgt

$$0 = \sum_{i:=1}^n m_i^\eta (x_i y)^\alpha = \sum_{i:=1}^n m_i (x_i a)^\alpha.$$

Also ist auch

$$0 = \sum_{i:=1}^n m_i \bigl(x_i y + (x_i y)^\alpha\bigr).$$

Weil M aus F-linear unabhängigen Vektoren besteht, folgt

$$0 = x_i y + (x_i y)^\alpha$$

für alle i und alle y. Wäre $x_j \neq 0$, so folgte mit $y := x_j^{-1}$, dass $0 = 1 + 1$ wäre. Mit $y := x_j^{-1} z$ folgte daher $0 = z + z^\alpha$ und dann $z^\alpha = z$. Dies widerspräche aber der Tatsache, dass α nicht die Identität ist. Damit ist 1) bewiesen.

2) Ist B eine F-Basis von W, so ist B eine K-Basis von V.

Wegen 1) genügt es zu zeigen, dass B ein K-Erzeugendensystem von V ist.

Es sei zunächst die Charakteristik von K von 2 verschieden. Nach 6.3 gibt es dann ein $j \in K$ mit $j^\alpha = -j$. Es folgt $(j^2)^\alpha = j^2$, so dass $j^2 \in F$ ist. Ferner ist V als abelsche Gruppe die direkte Summe von W und $W' := \{v \mid v \in V, v^\eta = -v\}$. Offensichtlich ist $Wj \subseteq W'$ und $W'j \subseteq W$, so dass $Wj^2 \subseteq W$ ist. Weil W ein F-Vektorraum ist und j^2 in F^* liegt, ist daher $Wj^2 = W$. Hieraus folgt

$$W = Wj^2 \subseteq W'j \subseteq W,$$

so dass $W'j = W$ ist. Hieraus folgt $V = W + Wj^{-1}$, so dass B in der Tat ein K-Erzeugendensystem von V ist.

Ist die Charakteristik von K gleich 2, so gibt es nach 6.3 ein $j \in K$ mit $j^\alpha = j + 1$. Ist $v \in V$, so ist $v + v^\eta \in W$ und

$$\big(v + (v + v^\eta)j\big)^\eta = v^\eta + (v + v^\eta)(j + 1) = v + (v + v^\eta)j,$$

so dass $v + (v + v^\eta)j \in W$ gilt. Aus $v = v + (v^\eta)j + (v + v^\eta)j$ folgt daher, dass $V = W + Wj$ ist. Also ist B auch in diesem Falle ein K-Erzeugendensystem von V.

3) Ist P ein Fixpunkt von σ, so ist $P \cap W$ ein F-Unterraum des Ranges 1 von W.

Es sei $P = pK$. Dann ist $p^\eta = pa$ mit einem $a \in K^*$. Ferner ist $p = p^{\eta^2} = paa^\alpha$, so dass $aa^\alpha = 1$. Nach 6.4 gibt es daher ein $c \in K^*$ mit $a = cc^{-\alpha}$. Setze $q := pc$. Dann ist $0 \neq q \in P$. Ferner ist

$$q^\eta = (pc)^\eta = p^\eta c^\alpha = pac^\alpha = pc = q.$$

Also ist $P \cap W \neq \{0\}$. Mit 1) folgt

$$\mathrm{Rg}_F(P \cap W) \leq \mathrm{Rg}_K(V),$$

so dass, wie behauptet, $\mathrm{Rg}_F(P \cap W) = 1$ ist.

4) Es sei L die Menge der Unterräume von $L_K(V)$, die von Fixpunkten von σ aufgespannt werden. Dann erbt L von $L_K(V)$ die Teilordnung. Definiert man die Abbildung φ von L in $L_F(W)$ durch $X^\varphi := X \cap W$ für alle $X \in L$, so ist φ ein Isomorphismus von L auf $L_F(W)$. Insbesondere ist L also ein projektiver Verband.

Es seien X, $Y \in L$. Ist $X \leq Y$, so ist

$$X^\varphi = X \cap W \leq Y \cap W = Y^\varphi.$$

Es sei umgekehrt $X^\varphi \leq Y^\varphi$. Die Definition von L liefert zusammen mit 3), dass

$$X = \sum_{x \in X^\varphi} xK \leq \sum_{y \in Y^\varphi} yK = Y$$

ist. Damit ist φ als Monomorphismus von L in $L_F(W)$ erkannt.

Es sei $Y \in L_F(W)$. Setze $X := \sum_{y \in Y} yK$. Wegen $(yK)^\eta = yK$ ist $X \in L$. Überdies ist $X^\varphi = X \cap W > Y$. Es sei $x \in X \cap W$. Es gibt dann $y_1, \ldots, y_n \in Y$ und $k_1, \ldots, k_n \in K$ mit $x = \sum_{i:=1}^n y_i k_i$. Wir dürfen annehmen, dass die y_i als Vektoren des K-Vektorraumes V linear unabhängig sind. Dann sind sie aber auch F-linear unabhängig. Somit lassen sie sich zu einer Basis von W ergänzen. Weil nach 2) jede F-Basis von W eine K-Basis von V ist, folgt aus $x \in W$, dass $k_1, \ldots, k_n \in F$ ist. Also ist $x \in Y$, so dass $X^\varphi = Y$ ist. Folglich ist φ ein Isomorphismus von L auf $L_F(W)$.

Es sei $\gamma \in \mathrm{G^*L}(V, K)$ und es gelte $v^{\gamma\eta} = v^{\eta\gamma}e$ für alle $v \in V$. Nach 6.1 ist dann entweder $e = 1$ oder $e = -1$. Weil die von γ in $L_K(V)$ induzierte Kollineation im Zentralisator C von σ liegt, ist $L^\gamma = L$. Daher ist $\varphi^{-1}\gamma\varphi$ eine Kollineation von $L_F(W)$. Wegen 2) ist $\mathrm{Rg}_F(W) \geq 3$. Nach dem zweiten Struktursatz

II.7.1 gibt es daher eine semilineare Abbildung (δ, β) des F-Vektorraumes W in sich, welche in $L_F(W)$ die Kollineation $\varphi^{-1}\gamma\varphi$ induziert. Hieraus folgt zusammen mit $\mathrm{Rg}_F(W) \geq 3$ die Existenz eines Elementes $a \in K^*$ mit $w^\delta = w^\gamma a$ für alle $w \in W$. Es ist

$$w^{\gamma\eta}a^\alpha = (w^\gamma a)^\eta = w^{\delta\eta} = w^\delta = w^{\eta\delta} = w^{\eta\gamma}a = w^{\gamma\eta}ea.$$

Also ist entweder $a^\alpha = a$ oder $a^\alpha = -a$. Ferner ist, falls $f \in F$ ist,

$$w^\delta f^\beta = (wf)^\delta = (wf)^\gamma a = w^\gamma fa = x^\delta a^{-1}fa.$$

Folglich ist $f^\beta = a^{-1}fa$ für alle $f \in F$. Ist $a^\alpha = a$, so ist $a \in F$, so dass wir auf Grund von 1.3 annehmen dürfen, dass $\beta = 1$ ist. Ist $a^\alpha = -a$ und ist $j \in K$ ein Element, für welches $j^\alpha = -j$ gilt, so ist $a = jf_0$ mit $f_0 \in F$ nach 6.3). Dann ist $f^\beta = f_0^{-1}j^{-1}fjf_0$, so dass wir wiederum nach 1.3 annehmen dürfen, dass $a = j$ ist. (Der Leser fragt sich vielleicht, warum so umständlich, wo doch $a^\alpha = -a$ gilt. Die Antwort lautet: Man kann j *a priori* wählen, und darauf kommt es an.) Es ist $-j = j^\alpha = kjk^{-1}$. Hieraus folgt, dass

$$k \neq -k = j^{-1}kj = k^\beta$$

ist. Nun ist F aber der Fixkörper von α, dh., der Zentralisator von k in K. Daher liegt k im Zentrum von F. Somit gilt nach dem Vorstehenden, dass β kein innerer Automorphismus von F ist. Es sei H das Urbild von C in $\mathrm{G^*L}(V, K)$. Ist dann $\gamma \in H$, so ist $v^{\gamma\eta} = v^{\eta\gamma}$ oder $v^{\gamma\eta} = -v^{\eta\gamma}$, wie wir schon bemerkten.

Es sei nun $\mathrm{Char}(K) = 2$. Dann ist $H = C_{\mathrm{PG^*L}(V,K)}(\eta)$. Daher ist $W^H = W$. Ist $\epsilon(\gamma)$ die Einschränkung von $\gamma \in H$ auf W, so ist ϵ ein Homomorphismus von H in $\mathrm{G^*L}(W, F)$. Weil jede F-Basis von W gleichzeitig eine K-Basis von V ist, ist ϵ injektiv. Es sei $\gamma \in \mathrm{G^*L}(W, F)$. Ist B eine F-Basis von W und definiert man die lineare Abbildung γ von V in sich durch $b^\gamma := b^\lambda$ für alle $b \in B$, so ist γ bijektiv und es gilt $\epsilon(\gamma) = \lambda$. Folglich ist ϵ ein Isomorphismus von H auf $\mathrm{G^*L}(W, F)$. Hieraus folgen nun die Behauptungen unter a).

Es sei schließlich $\mathrm{Char}(K) \neq 2$. Ferner sei B wieder eine F-Basis von W und j sei ein Element von K mit $j^\alpha = -j$. Ist nun $v \in V$ und $v = \sum_{b \in B} bx_b$ und definiert man γ durch $v^\gamma := \sum_{b \in B} bjx_b$, so ist $\gamma \in \mathrm{G^*L}(V, K)$. Überdies ist

$$v^{\gamma\eta} = \sum_{b \in B} b^\eta j^\alpha x_b^\alpha = -\sum_{b \in B} b_j x_b^\alpha = -(\sum_{b \in B} bx_b^\alpha)^\gamma = -v^{\eta\gamma}.$$

Daher ist $\gamma \in H$. Hieraus folgt, dass $H_0 := C_{\mathrm{G^*L}(V,K)}(\eta)$ den Index 2 in H hat. Weil $W \cap W^\gamma = \{0\}$ ist, folgt nach unserer Vorbemerkung, dass es eine bezüglich β semilineare Abbildung δ von W in sich gibt mit $w^\delta = w^\gamma j$ für alle $w \in W$. Weil β kein innerer Automorphismus ist, wird H_0 bei dem Homomorphismus von H auf C auf einen Normalteiler N vom Index 2 in C abgebildet. Ferner folgt ohne Mühe, wie schon im Falle der Charakteristik 2, dass $N/Z(N) \cong \mathrm{PG^*L}(W, F)$ und $Z(N) \cong Z(F^*)/Z(K^*)$ ist. Es bleibt zu zeigen, dass $Z(C)$ nur aus den beiden Elementen 1 und σ besteht.

Offensichtlich ist $Z(C) \subseteq Z(N)$. Es sei $1 \neq \rho \in Z(C)$ und ρ werde von ζ induziert. Es gibt dann ein $f \in Z(F^*)$ mit $w^\zeta = wf$ für alle $w \in W$. Weil β in $Z(F)$ einen Automorphismus der Ordnung 2 induziert und da $k^\beta = -k$ ist, gibt es nach 6.3 zwei Elemente $g, h \in Z(F)$ mit $f = g + kh$ und $g^\beta = g$ sowie $h^\beta = h$. Wegen $x^\beta = j^{-1}xj$ heißt das, dass g und h mit j vertauschbar sind. Weil g und h auch im Zentrum von F liegen und nach 6.3 die Gleichung $K = F + jF$ gilt, liegen g und h im Zentrum von K. Aus $\rho \neq 1$ folgt, dass $h \neq 0$ ist. Wir dürfen daher annehmen, dass $h = 1$ ist. Wegen $\rho \in Z(C)$ ist $v^{\zeta\gamma} = v^{\gamma\zeta}r$ mit einem passenden $r \in Z(K^*)$. Ist $b \in B$, so ist also

$$bjf = b^\gamma f = (bf)^\gamma = b^{\zeta\gamma} = b^{\gamma\zeta}r = b^\zeta jr = bfjr.$$

Somit ist, da ja $f = g + k$ ist,

$$j(g + k) = jf = fjr = gjr + kjr = jr(g - k).$$

Weil g in F und k nicht in F liegt, folgt $g = 0$ und $r = -1$. Somit ist

$$v^\zeta = \sum_{b\in B} b^\zeta x_b = \sum_{b\in B} bkx_b = \sum_{b\in B} b^\eta x_b^\alpha k = v^\eta k,$$

dh., es ist $\rho = \sigma$. Damit ist dann alles bewiesen.

Wir haben nun gute Kenntnisse über die Zentralisatoren von Involutionen, die keine Fixpunkte haben, und von Involutionen, die zwar Fixpunkte haben, die aber nicht durch involutorische lineare Abbildungen induziert werden. Für die noch verbleibenden projektiven Involutionen, die von involutorischen linearen Abbildungen induziert werden, ist die Arbeit aber auch schon erledigt, wie der nächste Satz zeigt.

6.6. Satz. *Es sei V ein Vektorraum über dem Körper K mit $\mathrm{Rg}_K(V) \geq 3$. Ist σ eine Kollineation von $L_K(V)$, die von einer involutorischen linearen Abbildung von V in sich induziert wird, so gilt:*
a) *Ist* $\mathrm{Char}(K) = 2$, *so ist σ eine Quasielation.*
b) *Ist* $\mathrm{Char}(K) \neq 2$, *so ist σ eine Quasistreckung.*

Der Beweis sei dem Leser als Übungsaufgabe überlassen.

7. Die hessesche Gruppe

Schlitzt man die projektive Ebene über GF(3) bezüglich einer Geraden, so erhält man die *affine Ebene* über GF(3). Diese ist eine Inzidenzstruktur aus 9 Punkten und 12 Geraden. Sie findet auch bei Anhängern der algebraischen Geometrie Interesse, da sie sich nämlich in vielen projektiven Ebenen — insbesondere in der über dem Körper der komplexen Zahlen — als Konfiguration der Wendepunkte einer irreduziblen Kurve dritten Grades wiederfindet. Der Stabilisator dieser Konfiguration in der projektiven Gruppe ist die nach Ludwig Otto Hesse benannte *hessesche Gruppe*. Eine Untergruppe dieser Gruppe wird im nächsten Abschnitt ihren Beitrag zur Länge der dort vorgeführten Argumentationskette

leisten, so dass in diesen Abschnitt ein wenig über diese Situation berichtet werden soll.

Hesse publizierte seine Ergebnisse im crelleschen Journal (Hesse 1844, 1847, Salmon 1850). Sie finden sich wiedergegeben in Jordans „Traité“ und in Nettos „Substitutionentheorie“ (Jordan, S. 302ff, Netto 1882, S. 232ff). Heutige Leser haben es bequemer, wenn sie sich an die Ausarbeitung der brieskornschen Vorlesungen des WS 1975/76 und des SS 1976 halten (Brieskorn und Knörrer o. J., S. 379–388).

Die Punkte der affinen Ebene über GF(3) kann man identifizieren mit den Paaren (x, y) mit x, $y \in \mathrm{GF}(3)$. Die Geraden werden dann durch inhomogene lineare Gleichungen beschrieben. Kodiert man das Paar (x, y) durch die Zahl $3x + y$, so werden die Punkte der affinen Ebene über GF(3) durch die Ziffern 0 bis 8 beschrieben und die Geraden durch die Spalten der folgenden Matrix.

$$\begin{matrix} 0\,1\,2 & 0\,1\,2 & 0\,1\,2 & 0\,3\,6 \\ 3\,4\,5 & 4\,5\,3 & 5\,3\,4 & 1\,4\,7 \\ 6\,7\,8 & 8\,6\,7 & 7\,8\,6 & 2\,5\,8 \end{matrix}$$

Wir gehen nun der Frage nach, unter welchen Bedingungen sich diese affine Ebene in eine gegebene projektive Ebene einbetten lässt. Diese Frage erscheint nach den vorstehenden Bemerkungen vielleicht nicht ganz so künstlich, wie sie zunächst klingen mag. Hinzukommt, wie schon gesagt, dass sie sich im nächsten Abschnitt zwangsläufig stellen wird.

7.1. Satz. *Es sei V ein Vektorraum des Ranges 3 über dem Körper K und b_0, b_1, b_2 sei eine Basis von V. Ferner sei t ein von 0 und 1 verschiedenes Element aus K. Wir definieren eine Abbildung P von $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ in die Punktmenge von $L_K(V)$ durch*

$$\begin{aligned} P_0 &:= b_0K, \\ P_3 &:= b_1K, \\ P_4 &:= b_2K, \\ P_7 &:= (b_0 + b_1 + b_2)K, \\ P_6 &:= (b_0 + b_1t)K, \\ P_2 &:= (b_0 + b_1t + b_2)K, \\ P_1 &:= (b_0t + b_1t + b_2)K, \\ P_8 &:= (b_0t + b_2)K, \\ P_5 &:= (b_0(t^2 - t + 1) + b_1t + b_2t)K. \end{aligned}$$

Genau dann ist P ein Monomorphismus der affinen Ebene der Ordnung 3 in $L_K(V)$, wenn

$$t^2 - t + 1 = 0$$

ist.

Beweis. Weil t von 0 und 1 verschieden ist, ist P injektiv. Es ist $P_0 = b_0K, P_3 = b_1K$ und $P_6 = (b_0 + b_1t)K$, so dass diese drei Punkte kollinear sind.

Es ist $P_1 = (b_0t + b_1t + b_2)K, P_4 = b_2K$ und $P_7 = (b_0 + b_1 + b_2)K$, so dass diese Punkte wegen $t \neq 1$ kollinear sind.

Es ist $P_2 = (b_0 + b_1t + b_2)K, P_5 = (b_0(t^2 - t + 1) + b_1t + b_2t)K$ und $P_8 = (b_0t + b_2)K$. Wegen

$$(b_0 + b_1t + b_2) + (b_0t + b_2)(t - 1) = b_0(t^2 - t + 1) + b_1t + b_2t$$

sind auch diese drei Punkte kollinear.

Es ist $P_0 = b_0K$, $P_4 = b_2K$ und $P_8 = (b_0t + b_2)K$, so dass diese Punkte kollinear sind.

Es ist $P_1 = (b_0t + b_1t + b_2)K$, $P_5 = (b_0(t^2 - t + 1) + b_1t + b_2t)K$ und $P_6 = (b_0 + b_1t)K$. Wegen

$$(b_0t + b_1t + b_2)t - (b_0 + b_1t)(t - 1) = b_0(t^2 - t + 1) + b_1t + b_2t$$

sind diese drei Punkte ebenfalls kollinear.

Es ist $P_2 = (b_0 + b_1t + b_2)K$, $P_3 = b_1K$ und $P_7 = (b_0 + b_1 + b_2)K$, so dass diese drei Punkte wegen $t \neq 1$ kollinear sind.

Es ist $P_0 = b_0K$, $P_5 = (b_0(t^2 - t + 1) + b_1t + b_2t)K$ und $P_7 = (b_0 + b_1 + b_2)K$, so dass diese Punkte wegen $t \neq 1$ kollinear sind.

Es ist $P_1 = (b_0t + b_1t + b_2)K$, $P_3 = b_1K$ und $P_8 = (b_0t + b_2)K$, so dass auch diese drei Punkte kollinear sind.

Es ist $P_2 = (b_0 + b_1t + b_2)K$, $P_4 = b_2K$ und $P_6 = (b_0 + b_1t)K$. Somit sind auch diese drei Punkte kollinear.

Bislang ist also noch nichts weiter geschehen. Doch nun finden wir die Bedingung, die t erfüllen muss, damit P ein Monomorphismus ist.

Es ist $P_3 = b_1K$, $P_4 = b_2K$ und $P_5 = (b_0(t^2 - t + 1) + b_1t + b_2t)K$. Damit diese drei Punkte kollinear sind, ist notwendig und hinreichend, dass es λ und μ in K gibt mit

$$b_0(t^2 - t + 1) + b_1t + b_2t = b_1\lambda + b_2\mu.$$

Somit sind diese drei Punkte genau dann kollinear, wenn $t^2 - t + 1 = 0$ ist. Diese Bedingung ist also notwendig dafür, dass P ein Monomorphismus ist. Sie ist aber auch hinreichend. Um dies einzusehen, sei $t^2 - t + 1 = 0$. Wir müssen dann nur noch zeigen, dass auch die Tripel P_0, P_1, P_2 und P_6, P_7, P_8 kollinear sind.

Es ist $P_0 = b_0K$, $P_1 = (b_0t + b_1t + b_2)K$ und $P_2 = (b_0 + b_1t + b_2)K$. Wegen $t^2 - t + 1 = 0$ ist

$$b_0 = -(b_0t + b_1t + b_2)t + (b_0 + b_1t + b_2)t,$$

so dass auch diese Punkte kollinear sind.

Schließlich ist $P_6 = (b_0 + b_1t)K$, $P_7 = (b_0 + b_1 + b_2)K$ und $P_8 = (b_0t + b_2)K$. Nun ist aber

$$b_0 + b_1t = (b_0 + b_1 + b_2)t - (b_0t + b_2)t,$$

so dass auch dieses letzte Punktetripel kollinear ist. Damit ist der Satz bewiesen.

Die in Satz 7.1 beschriebene Einbettung der affinen Ebene über GF(3) in eine desarguessche projektive Ebene ist im Wesentlichen auch die einzige Möglichkeit, diese affine Ebene in eine desarguessche projektive Ebene einzubetten. Dies ist die Aussage des nächsten Satzes.

7.2. Satz. *Es sei V ein Vektorraum des Ranges 3 über dem Körper K. Ist dann P ein Monomorphismus der affinen Ebene über* GF(3) *in $L_K(V)$, so gibt es eine Basis b_0, b_1, b_2 von V sowie ein $t \in K$, so dass P mittels dieser Daten wie in Satz 7.1 beschrieben dargestellt ist. Insbesondere gibt es genau dann einen Monomorphismus der affinen Ebene über* GF(3) *in $L_K(V)$, wenn es ein $t \in K$ gibt mit $t^2 - t + 1 = 0$.*

Beweis. Da die Punkte P_0, P_3, P_4, P_7 einen Rahmen von $L_K(V)$ bilden, gibt es nach 1.8 Vektoren b_0, b_1, b_2 mit $P_0 = b_0K$, $P_3 = b_1K$, $P_4 = b_2K$ und $P_7 = (b_0 + b_1 + b_2)K$. Wegen $P_6 \leq P_0 + P_3$ und $P_6 \neq P_3$ gibt es ein $t \in K$ mit $P_6 = (b_0 + b_1t)K$. Nun ist

$$\begin{aligned} P_2 &= (P_3 + P_7) \cap (P_4 + P_6), \\ P_1 &= (P_4 + P_7) \cap (P_0 + P_2), \\ P_8 &= (P_0 + P_4) \cap (P_1 + P_3), \\ P_5 &= (P_1 + P_6) \cap (P_2 + P_8). \end{aligned}$$

Hieraus folgt alles weitere.

7.3. Satz. *Es sei V ein Vektorraum des Ranges 3 über dem Körper K. Es sei b_1, b_2, b_3 eine Basis von V und t sei ein Element in K mit $t^2 - t + 1 = 0$. Schließlich sei P der in 7.1 beschriebene Monomorphismus der affinen Ebene über* GF(3) *in $L_K(V)$. Mit C bezeichnen wir den Zentralisator von t in K^*. Ist dann $\sigma \in \mathrm{GL}(V)$, so gilt $P_i^\sigma = P_i$ für alle i genau dann, wenn es ein $\lambda \in C$ gibt mit $b_j^\sigma = b_j\lambda$ für $j := 0, 1, 2$. Die Gruppe der projektiven Kollineationen, die alle Punkte P_i festlassen, ist isomorph zu $C/Z(K^*)$.*

Beweis. Ist $\lambda \in C$ und gilt $b_j^\sigma = b_j\lambda$ für $j := 0, 1, 2$, so ist natürlich $P_i^\sigma = P_i$ für alle i. Es sei also $P_i^\sigma = P_i$ für alle i. Weil σ den Rahmen P_0, P_3, P_4, P_7 festlässt, gibt es ein $\lambda \in K^*$ mit $b_j^\sigma = b_j\lambda$ für $j := 0, 1, 2$. Mit $P_6^\sigma = P_6$ folgt die Existenz eines $\mu \in K^*$ mit

$$b_0\lambda + b_1\lambda t = (b_0 + b_1t)^\sigma = (b_0 + b_1t)\mu.$$

Hieraus folgt $\lambda = \mu$ und weiter $\lambda t = t\lambda$, so dass $\lambda \in C$ gilt. Damit ist die erste Aussage des Satzes bewiesen. Die zweite Aussage folgt unmittelbar aus der ersten.

Die Kollineationsgruppe der affinen Ebene über GF(3) ist schnell bestimmt. Nach I.8.8 lässt sich jede Kollineation dieser Ebene auf genau eine Weise zu einer Kollineation der projektiven Ebene über GF(3) fortsetzen. Daher ist die Kollineationsgruppe der affinen Ebene gleich dem Stabilisator einer Geraden in der Kollineationsgruppe der projektiven Ebene. Mit 1.13 folgt daher, dass diese Gruppe die Ordnung $3^3 \cdot 2^4$ hat. Sie enthält den Normalteiler der Ordnung

9, der aus den Elationen besteht, deren Achse die entfernte Gerade ist. Diese Elationen heißen in diesem Zusammenhang *Translationen*. Die Faktorgruppe nach dem Normalteiler der Translationen ist isomorph zur $\mathrm{GL}(2,3)$, wobei diese Gruppe innerhalb der Kollineationsgruppe sich als der Stabilisator eines Punktes der affinen Ebene wiederfindet. Wir wollen uns nun überlegen, was von diesen Kollineationen bei der Einbettung der affinen Ebene über $\mathrm{GF}(3)$ in eine desarguessche projektive Ebene im Stabilisator der eingebetteten Ebene in der projektiven Gruppe der einbettenden Ebene wiederzufinden ist.

7.4. Satz. *Es sei K ein Körper und t ein Element aus K mit $t^2-t+1=0$. Es sei ferner V ein Vektorraum vom Rang 3 über K und b_0, b_1, b_2 sei eine Basis von V. Schließlich sei P der in 7.1 mittels dieser Daten definiert Monomorphismus der affinen Ebene der Ordnung 3 in $L_K(V)$. Wir definieren die Abbildungen ρ, σ und τ in $\mathrm{GL}(V)$ durch*

$$\begin{aligned}
b_0^\rho &:= -b_0\\
b_1^\rho &:= b_0t^{-1}+b_1\\
b_2^\rho &:= b_0t+b_2,\\
b_0^\sigma &:= b_0+b_1t\\
b_1^\sigma &:= -b_1\\
b_2^\sigma &:= b_1+b_2,\\
b_0^\tau &:= b_0+b_2t^{-1}\\
b_1^\tau &:= b_1+b_2\\
b_2^\tau &:= -b_2.
\end{aligned}$$

Dann sind ρ, σ und τ Involutionen, die in $L_K(V)$ involutorische Perspektivitäten induzieren. Nennt man diese wiederum ρ, σ und τ, so gilt:

Das Zentrum von ρ ist P_0, die Achse ist

$$\bigl\{b_0\lambda_0+b_1(2t\lambda_0-t^2\lambda_2)+b_2\lambda_2 \mid \lambda_0,\lambda_2\in K\bigr\}$$

und ρ wirkt auf den P_i durch $(P_1P_2)(P_3P_6)(P_4P_8)(P_5P_7)$.

Das Zentrum von σ ist P_3, die Achse ist

$$\bigl\{b_0\lambda_0+b_1\lambda_1+b_2(2\lambda_1-t\lambda_2) \mid \lambda_0,\lambda_1\in K\bigr\}$$

und σ wirkt auf den P_i durch $(P_0P_6)(P_1P_8)(P_2P_7)(P_4P_5)$.

Das Zentrum von τ ist P_4, die Achse ist

$$\bigl\{b_0(2t\lambda_2-t\lambda_1)+b_1\lambda_1+b_2\lambda_2 \mid \lambda_1,\lambda_2\in K\bigr\}$$

und τ wirkt auf den P_i durch $(P_0P_8)(P_1P_7)(P_2P_6)(P_3P_5)$.

Die von ρ, σ und τ erzeugte Kollineationsgruppe induziert auf der affinen Ebene der Ordnung drei eine Gruppe der Ordnung $9\cdot 2$ bestehend aus den Translationen und Streckungen dieser Ebene.

Beweis. Dies zu beweisen ist eine banale Rechenaufgabe.

7.5. Satz. *Es sei K ein Körper und t sei ein Element aus K mit $t^2 - t + 1 = 0$. Es sei ferner V ein Vektorraum vom Rang 3 über K und b_0, b_1, b_2 sei eine Basis von V. Schließlich sei P der in 7.1 mittels dieser Daten definierte Monomorphismus der affinen Ebene der Ordnung 3 in $L_K(V)$. Wir definieren die Abbildungen ρ und σ in $\mathrm{GL}(V)$ durch*

$$\begin{aligned}
b_0^\rho &:= b_0(t-1)\\
b_1^\rho &:= b_1(t-1)\\
b_2^\rho &:= b_0 + b_1 + b_2,\\
b_0^\sigma &:= b_0(t-1)\\
b_1^\sigma &:= -(b_0 + b_1 + b_2)t\\
b_2^\sigma &:= b_2(t-1).
\end{aligned}$$

Dann sind ρ und σ Elemente der Ordnung 3. Die von ihnen in $L_K(V)$ induzierten Kollineation lassen die durch P beschriebene affine Ebene invariant. Bezeichnet man diese Kollineationen ebenfalls mit ρ und σ, so gilt:

Die Kollineation ρ hat die Fixpunkte P_0, P_3 und P_6 und die Wirkung von ρ auf den restlichen Punkten wird durch

$$(P_1P_4P_7)(P_2P_8P_5)$$

beschrieben.

Die von diesen beiden Kollineationen erzeugte Gruppe induziert auf der affinen Ebene der Ordnung 3 eine zur $\mathrm{SL}(2,3)$ isomorphe Gruppe.

Beweis. Auch dies ist banal zu verifizieren.

Die beiden Sätze 7.4 und 7.5 implizieren, dass der Stabilisator der Menge der Punkte der P_i auf dieser Menge zweifach transitiv operiert.

Geraden einer affinen Ebene, deren Schnittpunkt in der zugehörigen projektiven Ebene auf der entfernten Gerade liegt, heißen *parallel*. Die Parallelitätsrelation ist eine Äquivalenzrelation. Ihre Äquivalenzklassen heißen *Parallelenscharen*.

7.6. Satz. *Es sei K ein Körper und t sei ein Element aus K mit $t^2-t+1=0$. Es sei ferner V ein Vektorraum vom Rang 3 über K und b_0, b_1, b_2 sei eine Basis von V. Schließlich sei P der in 7.1 mittels dieser Daten definierte Monomorphismus der affinen Ebene der Ordnung 3 in $L_K(V)$. Das Bild dieser affinen Ebene unter P werde mit α bezeichnet. Dann sind die folgenden Aussagen äquivalent:*

a) *Es ist $t = -1$.*
b) *Die Charakteristik von K ist gleich 3.*
c) *Die Geraden einer jeden Parallelschar von α sind als Geraden von $L_K(V)$ konfluent.*
d) *Es gibt eine Parallelenschar in α, deren Geraden als Geraden von $L_K(V)$ konfluent sind.*

Beweis. a) und b) sind äquivalent: Ist $t = -1$, so ist $0 = t^2 - t + 1 = 3$, so dass b) eine Folge von a) ist. Ist die Charakteristik von K gleich 3, so ist $0 = t^2 - t + 1 = (t+1)^2$, da ja $-1 = 2$ ist. Folglich ist $t = -1$.

b) impliziert c): Da die Charakteristik von K gleich 3 ist, enthält $L_K(V)$ auch eine Kopie der projektiven Ebene über GF(3). Da -1 die einzige Lösung der Gleichung $t^2 - t + 1 = 0$ ist, folgt mit 7.2 die Gültigkeit von c).

c) ist zu d) äquivalent: Aus c) folgt natürlich d). Weil der Stabilisator von α in der projektiven Gruppe von $L_K(V)$ auf der Punktmenge von α zweifach transitiv operiert, ist c) auch eine Konsequenz von d).

c) impliziert b): Es ist $(b_0+b_1)K = (P_0+P_3)\cap(P_4+P_7)$. Nach Voraussetzung ist $(b_0 + b_1)K \leq P_2 + P_5$. Es gibt also r, $s \in K$ mit $b_0 + b_1 = (b_0 + b_1 t + b_2)r + (b_1 + b_2)s$. Hieraus folgen die Gleichungen $r = 1$, $tr - s = 1$ und $s + r = 0$. Hieraus folgt $t = 2$ und weiter $0 = t^2 - t + 1 = 3$. Damit ist alles bewiesen.

7.7. Satz. *Es sei K ein Körper und t sei ein Element aus K mit $t^2 - t + 1 = 0$, sei ferner V ein Vektorraum vom Rang 3 über K und b_0, b_1, b_2 sei eine Basis von V. Schließlich sei P der in 7.1 mittels dieser Daten definierte Monomorphismus der affinen Ebene der Ordnung 3 in $L_K(V)$. Das Bild dieser affinen Ebene unter P werde mit α bezeichnet und G sei der Stabilisator von α in $\mathrm{PGL}(V)$.*

a) *Ist die Charakteristik von K gleich 3, so induziert G die volle Kollineationsgruppe in der affinen Ebene α.*

b) *Ist die Charakteristik von K von 3 verschieden, so induziert G in α die Gruppe $T \cdot SL(2,3)$, wobei T die Gruppe der Translationen von α bezeichnet. Diese Gruppe ist vom Index 2 in der vollen Kollineationsgruppe von α.*

Beweis. a) ist banal.

b) Die Gruppe, die von G auf α induziert wird, enthält die Gruppe $T \cdot \mathrm{SL}(2,3)$, wie wir früher schon feststellten. Diese Gruppe ist vom Index 2 in der vollen Kollineationsgruppe von α. Es genügt also, eine Kollineation von α aufzuzeigen, die nicht durch eine Kollineation aus G induziert wird.

Die affine Ebene α besitzt eine involutorische Kollineation, die die Punkte P_0 P_3 und P_6 festlässt und die P_4 auf P_8 abbildet. Wir nehmen an, dass diese Kollineation durch eine Kollineation $\tau \in G$ induziert werde. Es gibt dann ein mit t vertauschbares Element $\lambda \in K^*$ mit $b_0^\tau = b_0\lambda$ und $b_1^\tau = b_1\lambda$ sowie ein $\mu \in K^*$ mit $b_2^\tau = (b_0 t + b_2)\mu$. Weil τ involutorisch ist, gibt es ein $\nu \in K^*$ mit

$$b_2\nu = b_2^{\tau^2} = b_0(\lambda t\mu + t\mu^2) + b_2\mu^2.$$

Weil λ mit t vertauschbar ist, folgt

$$0 = \lambda t\mu + t\mu^2 = t(\lambda\mu + \mu^2),$$

so dass $\mu = -\lambda$ ist. Also ist $b_2^\tau = -(b_0 t + b_2)\lambda$. Weiter folgt $P_7^\tau = P - 2$. Es gibt daher ein $\kappa \in K^*$ mit

$$(b_0 + b_1 t + b_2)\kappa = (b_0 + b_1 + b_2)^\tau = b_0(\lambda - t\lambda) + b_1\lambda - b_2\lambda.$$

Hieraus folgt $\kappa = \lambda - t\lambda$, $t\kappa = \lambda$ und $\kappa = -\lambda$ und dann $t = -1$, so dass nach 7.6 die Charakteristik von K gleich 3 ist. Dies widerspricht aber unserer Annahme. Damit ist der Satz bewiesen.

Im Falle der Charakteristik 3 ist nichts außergewöhnlich an der bislang betrachteten Situation. Wir werden sie daher im nächsten Satz ausschließen. In ihm studieren wir die Einbettung einer affinen Ebene der Ordnung 3 in eine pappossche projektive Ebene, da in einer solchen Ebene die Verhältnisse besonders einfach sind.

7.8. Satz. *Es sei K ein kommutativer Körper mit von 3 verschiedener Charakteristik und t sei ein Element aus K mit $t^2 - t + 1 = 0$. Es sei ferner V ein Vektorraum vom Rang 3 über K und b_0, b_1, b_2 sei eine Basis von V. Schließlich sei P der in 7.1 mittels dieser Daten definierte Monomorphismus der affinen Ebene der Ordnung 3 in $L_K(V)$. Das Bild dieser affinen Ebene unter P werde mit α bezeichnet und G sei der Stabilisator von α in $\mathrm{PGL}(V)$. Dann enthält G einen Normalteiler T der Ordnung 9 und G/T ist zur $\mathrm{SL}(2,3)$ isomorph. Darüber hinaus gilt $T = C_{\mathrm{PGL}(V)}(T)$.*

Beweis. Weil K kommutativ ist, ist $L_K(V)$ pappossch, so dass mit 1.11 folgt, dass G auf α treu operiert. Mit 7.7 b) folgt daher die erste Aussage über die Gruppe G. Es seien ρ und σ die unter diesen Namen in 7.4 definierten Abbildungen. Bezeichnet man die von diesen Abbildungen induzierten Kollineationen ebenfalls mit ρ bzw. σ, so folgt $\rho\sigma \in T$. Ferner gilt

$$\begin{aligned}
b_0^{\rho\sigma} &= -b_0 - b_1 t \\
b_1^{\rho\sigma} &= b_0 t^{-1} \\
b_2^{\rho\sigma} &= b_0 t + b_1 t + b_2.
\end{aligned}$$

Nun ist $(b_0 r_0 + b_1 r_2 + b_2 r_2)K$ genau dann ein Fixpunkt von $\rho\sigma$, wenn es ein $\mu \in K^*$ gibt mit

$$\begin{aligned}
r_0 \mu &= -r_0 + t^{-1} r_1 + t r_2 \\
r_1 \mu &= -t r_0 + t r_2 \\
r_2 \mu &= r_2.
\end{aligned}$$

Es sei zunächst $r_2 = 0$. Dann ist $r_0 \neq 0$, da andernfalls auch $r_1 = 0$ wäre. Ferner ist

$$r_0 \mu^2 = -r_0 \mu + t^{-1} r_1 \mu = -r_0 \mu + t^{-1}(-t r_0) = -r_0(\mu + 1).$$

Wegen $r_0 \neq 0$ folgt $\mu^2 + \mu + 1 = 0$.

Ist umgekehrt $\mu \in K$ und $\mu^2 + \mu + 1 = 0$, so ist $(b_0 - b_1 t \mu^{-1})K$ ein Fixpunkt von $\rho\sigma$, wie man leicht nachprüft.

Weil K kommutativ ist, hat das Polynom $x^2 + x + 1$ höchstens zwei Nullstellen. Eine davon ist $-t$. Da die Charakteristik von K von drei verschieden ist, ist $-t$ eine primitive dritte Einheitswurzel, so dass t^2 die zweite Nullstelle ist. Somit sind $(b_0 + b_1)K$ und $(b_0 - b_1 t^{-1})K$ zwei Fixpunkte von $\rho\sigma$.

Für jeden weiteren Fixpunkt dürfen wir $r_2 = 1$ annehmen. Dann ist auch $\mu = 1$ und somit

$$\begin{aligned}
r_0 &= -r_0 + t^{-1} r_1 + t \\
r_1 &= -t r_0 + t
\end{aligned}$$

Hieraus folgt $r_0 = 1 + t$. Weil die Charakteristik nicht 3 ist, gibt es also noch genau einen weiteren Fixpunkt, so dass $\rho\sigma$ genau drei Fixpunkte hat. Weil die von 1 verschiedenen Elemente von T in G alle konjugiert sind, haben sie alle genau drei Fixpunkte.

Es sei nun γ aus dem Zentralisator von T. Da γ mit jedem Element von T vertauschbar ist, permutiert γ die drei Fixpunkte eines jeden von 1 verschiedenen Elementes von G unter sich. Hieraus folgt, dass α von γ festgelassen wird, so dass $\gamma \in G$ gilt. In G ist T aber sein eigener Zentralisator. Damit ist alles bewiesen.

Erst als wir μ mit $-t$ bzw. t^2 identifizierten, haben wir von der Kommutativität von K Gebrauch gemacht. Dies zeigt, dass es im Nichtkommutativen Kollineationen mit ungewohnten Fixpunktkonfigurationen gibt. Dies ist die eine Bemerkung, die zu 7.8 zu machen ist. Die andere ist die, dass G im Falle eines nicht kommutativen Körpers nicht treu auf α operiert. Dies hat zur Folge, dass T nicht sein eigener Zentralisator ist.

Dieser Abschnitt führt den Namen *hessesche Gruppe* im Titel, so dass zum Schluß noch einmal gesagt sein soll, dass sich unter diesem Namen die Gruppe G des Satzes 7.8 verbirgt.

8. Isomorphismen der großen projektiven Gruppe

Ist σ ein Isomorphismus oder ein Antiisomorphismus von $L_K(V)$ auf $L_{K'}(V')$ und definiert man φ durch $\gamma^\varphi := \sigma^{-1}\gamma\sigma$ für alle $\gamma \in \mathrm{PG^*L}(V)$, so ist φ, falls $\mathrm{Rg}_K(V) \geq 3$ ist, ein Isomorphismus von $\mathrm{PG^*L}(V)$ auf $\mathrm{PG^*L}(V')$, da σ wegen $\mathrm{Rg}_K(V) \geq 3$ nach den Struktursätzen durch eine semilineare Abbildung von V auf V', bzw. von V auf V'^*, aufgefasst als Vektorraum über $K_\circ$, induziert wird. Wir werden in diesem Abschnitt zeigen, dass auch umgekehrt jeder Isomorphismus von $\mathrm{PG^*L}(V)$ auf $\mathrm{PG^*L}(V')$ durch einen Isomorphismus oder Antiisomorphismus von $L_K(V)$ auf $L_{K'}(V')$ induziert wird, falls nur $\mathrm{Rg}_K(V) \geq 3$ und $\mathrm{Rg}_{K'}(V') \geq 3$ ist. Hat wenigstens eine der beiden projektiven Geometrien den Rang 2, so gilt dieser Sachverhalt nicht mehr, wie die Ausnahmeisomorphismen zeigen. Man kann jedoch mehr zeigen, als wir hier tun, muss sich dann aber anderer Beweismethoden bedienen. Mehr zu diesem Thema findet sich in Dieudonné (1955).

Es sei daran erinnert, dass wir mit $\mathrm{E}(X, Y)$ die Gruppe aller Quasielationen bezeichnen, deren Zentren in X liegen und deren Achsen Y enthalten. Ist $X = Y$, so schreiben wir abkürzend $\mathrm{E}(X)$ an Stelle von $\mathrm{E}(X, Y)$.

8.1. Satz. *Es sei V ein Vektorraum über dem Körper K mit $\mathrm{Rg}_K(V) \geq 3$. Ferner sei G eine Gruppe von Elationen von $L_K(V)$. Genau dann gilt $G = \mathrm{E}(U)$, wobei U entweder ein Punkt oder eine Hyperebene von $L_K(V)$ ist, wenn $G = C_{\mathrm{PG^*L}(V)}(G)$ ist.*

Beweis. Es sei $G = \mathrm{E}(U)$ und U sei eine Hyperebene von $L_K(V)$. Weil $\mathrm{E}(U)$ abelsch ist, ist $G \subseteq C_{\mathrm{PG^*L}(V)}(G)$. Es sei $\gamma \in C_{\mathrm{PG^*L}(V)}(G)$. Ist P Zentrum einer von Eins verschiedenen Elation aus G, so ist $P^\gamma = P$. Folglich ist γ eine Perspektivität mit der Achse H. Weil $\mathrm{E}(U)$ auf der Menge der nicht in U

liegenden Punkte transitiv operiert, ist $\gamma = 1$, falls γ einen Fixpunkt außerhalb U hat. Also ist $\gamma \in \mathrm{E}(U) = G$. Dies zeigt, dass $G = C_{\mathrm{PG^*L}(V)}(G)$ ist.

Ist U ein Punkt und ist $G = \mathrm{E}(U)$, so zeigt man entsprechend, dass $G = C_{\mathrm{PG^*L}(V)}(G)$ ist.

Es sei nun umgekehrt $G = C_{\mathrm{PG^*L}(V)}(G)$. Dann ist G insbesondere abelsch. Außerdem ist $G \neq \{1\}$. Es sei U der von den Zentren der Elemente aus $G - \{1\}$ aufgespannte Unterraum und W sei der Schnitt der Achsen der Elationen aus $G - \{1\}$. Ist P Zentrum der Elation $\sigma \in G - \{1\}$ und ist H die Achse einer Elation $\tau \in G - \{1\}$, so folgt aus $\sigma\tau = \tau\sigma$, dass $P \leq H$ ist. Also ist $U \leq W$. Dies hat $G \subseteq \mathrm{E}(U, W)$ zur Folge. Nach 5.6 ist $\mathrm{E}(U, W)$ abelsch, so dass $G = \mathrm{E}(U, W)$ gilt. Es sei P ein Punkt auf W und H eine Hyperebene, die $U + P$ enthalte. Dann ist $\mathrm{E}(P, H) \subseteq C_{\mathrm{PG^*L}(V)}(G) = G$. Hieraus folgt $P \leq U$ und $W \leq H$. Dies impliziert $U = W$. Wäre nun U weder ein Punkt noch eine Hyperebene, so gäbe es eine Gerade X und eine Ko-Gerade Y mit $X \leq U \leq Y$. Ferner gäbe es ein $\alpha \in \mathrm{Hom}_K(V, X)$ mit $V^\alpha = X$ und $\mathrm{Kern}(\alpha) = Y$. Definierte man τ vermöge $v^\tau := v + v^\alpha$, so wäre $\tau \in \mathrm{E}(U) = G$. Es folgte der Widerspruch $\mathrm{Rg}_K(X) = 1$, da G ja eine Gruppe von Elationen ist. Dieser Widerspruch zeigt, dass U eine Punkt oder eine Hyperebene ist.

8.2. Satz. *Es sei V ein Vektorraum über dem Körper K und der Rang von V sei mindestens 3. Ferner sei G eine Untergruppe von $\mathrm{PG^*L}(V)$ und σ eine involutorische Streckung von $L_K(V)$. Gilt*

a) *Die Gruppe G enthält keine Involution,*

b) *Es ist $G = C_{\mathrm{PG^*L}(V)}(G)$,*

c) *Ist $\gamma \in G$, so gibt es ein $\eta \in G$ mit $\gamma\sigma = \eta^{-1}\sigma\eta$,*

so gilt eine der folgenden Aussagen:

1) *Es gibt eine Hyperebene H von $L_K(V)$ mit $G = \mathrm{E}(H)$.*

2) *Es gibt einen Punkt P von $L_K(V)$ mit $G = \mathrm{E}(P)$.*

3) *Es ist $\mathrm{Rg}_K(V) = 3$, die Gruppe G ist endlich und hat die Ordnung 9 und die Zentren der involutorischen Streckungen aus GZ, wobei $Z := \{1, \sigma\}$ gesetzt wird, sind die Punkte einer affinen Unterebene der Ordnung 3 von $L_K(V)$.*

Beweis. Nach c) ist $\gamma\sigma$ eine involutorische Streckung. Daher ist $(\gamma\sigma)^2 = 1$ und folglich $\sigma\gamma\sigma = \gamma^{-1}$. Ist $Z := \{1, \sigma\}$, so ist also $M := GZ$ eine Gruppe. Ferner folgt aus $\gamma = \gamma\sigma\sigma$, dass M von den Elementen $\gamma\sigma$ mit $\gamma \in G$ erzeugt wird.

Es seien γ und δ zwei verschiedene Elemente aus G. Haben $\gamma\sigma$ und $\delta\sigma$ beide das Zentrum P, so ist

$$\gamma\delta^{-1} = \gamma\sigma\delta\sigma$$

eine Perspektivität mit dem Zentrum P. Weil $\gamma\delta^{-1}$ von G nach b) zentralisiert wird, folgt, dass P unter G festbleibt. Daher haben wegen c) alle involutorischen Streckungen in M das Zentrum P. Hieraus folgt, da die involutorischen Streckungen ja M erzeugen, dass alle Elemente aus M Perspektivitäten mit dem Zentrum P sind. Es sei $1 \neq \gamma \in G$ und H sei die Achse von γ. Weil G abelsch ist, folgt $H^G = H$. Wegen $\sigma^{-1}\gamma\sigma = \sigma\gamma\sigma = \gamma^{-1}$ gilt auch $H^\sigma = H$. Läge P nicht auf H, so wäre M eine Untergruppe von $\Delta(P, H)$. Da diese Gruppe zur

multiplikativen Gruppe von K isomorph wäre, enthielte M nur eine Involution. Hieraus folgt $\gamma\sigma = \sigma$ für alle $\gamma \in G$, so dass $G = \{1\}$ wäre. Dieser Widerspruch zu b) zeigt, dass $P \leq H$ ist. Somit ist G eine Gruppe von Elationen, so dass in diesem Falle mit 8.1 die Aussage 1) folgt.

Haben $\gamma\sigma$ und $\delta\sigma$ beide die Achse H, so sieht man ganz entsprechend, dass $G = \mathrm{E}(H)$ ist, dh., dass die Aussage 2) gilt.

Wir nehmen nun an, dass für alle verschiedenen γ und δ in G die Kollineationen $\gamma\sigma$ und $\delta\sigma$ verschiedene Zentren und verschiedene Achsen haben. Mit C_γ bezeichnen wir das Zentrum und mit H_γ die Achse von $\gamma\sigma$. Ferner setzen wir

$$A := \sum_{\gamma \in G - \{1\}} C_\gamma \qquad \text{und} \qquad B := \bigcap_{\gamma \in G - \{1\}} H_\gamma.$$

Dann gilt:

(1) Es ist $A = V$ oder $B = \{0\}$.

Ist nämlich $A \neq V$ und $B \neq \{0\}$, so gibt es einen Punkt $P \leq B$ und eine Hyperebene H mit $A \leq H$. Ist dann ρ eine von 1 verschiedene Perspektivität mit dem Zentrum P und der Achse H, so ist $C_\gamma^\rho = C_\gamma$ und $H_\gamma^\rho = H_\gamma$ für alle $\gamma \in G$. Weil es in $\Delta(C_\gamma, H_\gamma)$ nur eine involutorische Perspektivität gibt, folgt weiter $\rho^{-1}\gamma\sigma\rho = \gamma\sigma$ für alle $\gamma \in G$. Weil M von den Elementen $\gamma\sigma$ erzeugt wird, folgt schließlich

$$\rho \in C_{\mathrm{PG^*L}(V)}(M) \subseteq C_{\mathrm{PG^*L}(V)}(G) = G.$$

Hieraus folgt $\rho = \sigma^{-1}\rho\sigma = \rho^{-1}$ im Widerspruch zu a).

(2) Die Gruppe G operiert auf $\{C_\gamma \mid \gamma \in G\}$ und auf $\{H_\gamma \mid \gamma \in G\}$ regulär.

Da G ja abelsch ist und $\sigma\eta = \eta^{-1}\sigma$ für alle $\eta \in G$ gilt, ist

$$\eta^{-1}\gamma\sigma\eta = \eta^{-2}\gamma\sigma$$

für alle γ, $\eta \in G$. Also ist $C_\gamma^\eta = C_{\eta^{-2}\gamma}$ und $H_\gamma^\eta = H_{\eta^{-2}\gamma}$. Weil die Abbildungen C und H injektiv sind, folgt (2) somit aus a).

Es sei $1 \neq \gamma \in G$. Dann lässt γ wegen $\gamma = \gamma\sigma\sigma$ die Gerade $X := C_1 + C_\gamma$ hyperebenenweise und die Ko-Gerade $Y := H_1 \cap H_\gamma$ punktweise fest. Für dieses γ gelten die nächsten beiden Aussagen.

(3) Es gibt ein $\eta \in G$ mit $X^\eta \neq X$ oder $Y^\eta \neq Y$.

Andernfalls wäre $X^G = X$ und $Y^G = Y$. Aus c) und $\mathrm{Rg}_K(V) \geq 3$ folgte dann, dass $A = X \neq V$ und $B = Y \neq \{0\}$ wäre im Widerspruch zu (1).

(4) Alle Fixpunkte von γ, die nicht in Y liegen, liegen auf X und alle Fixhyperebenen von γ, die X nicht enthalten, enthalten Y.

Es sei F ein Fixpunkt von γ, der nicht in Y liege. Aus (2) folgt, dass weder C_1 noch C_γ ein Fixpunkt von γ ist, so dass F von diesen beiden Punkten verschieden ist. Wäre $F \leq H_1$, so wäre $H_1 = F + Y$ und daher $H_1^\gamma = H_1$ im Widerspruch zu (2). Also ist $F \not\leq H_1$. Ebenso folgt $F \not\leq H_\gamma$. Daher ist $F \neq F^\sigma$ und $F \neq F^{\gamma\sigma}$. Es folgt weiter $C_1 \leq F + F^\sigma$ und $C_\gamma \leq F + F^{\gamma\sigma}$. Nun ist $F = F^\gamma$ und folglich $F^\sigma = F^{\gamma\sigma}$. Also ist

$$X = C_1 + C_\gamma \leq F + F^\sigma$$

und damit $X = F + F^\sigma$, so dass $F \leq X$ gilt.

Die zweite Aussage von (4) beweist sich analog.

(5) Es ist $\mathrm{Rg}_K(V) = 3$.

Es sei $\mathrm{Rg}_K(V) \geq 4$. Dann ist $\mathrm{Rg}_K(Y) \geq 2$. Nach (3) gibt es ein $\eta \in G$ mit $X^\eta \neq X$ oder $Y^\eta \neq Y$. Es sei $Y^\eta \neq Y$. Die Punkte von Y^η, die nicht in Y liegen, spannen Y^η auf. Überdies sind diese Punkte Fixpunkte von γ, da G ja abelsch ist. Hieraus und aus (4) folgt, dass $Y^\eta \leq X$ ist. Wegen $\mathrm{Rg}_K(X) = 2$ und $\mathrm{Rg}_K(Y) \geq 2$ ist daher $Y^\eta = X$. Weil die Punkte von Y^η Fixpunkte von γ sind und $C_1 \leq X = Y^\eta$ ist, ist $C_1^\gamma = C_1$. Dies widerspricht aber (2). Also ist $Y = Y^\eta$ und daher $X^\eta \neq X$. Weil G abelsch ist, lässt γ die Gerade X^η hyperebenenweise fest. Nach I.5.3 ist X^η die untere Grenze der es umfassenden Hyperebenen und es folgt, dass X^η die untere Grenze derjenigen Hyperebenen ist, die X^η aber nicht X umfassen. Mit (4) folgt daher, dass $Y \leq X^\eta$ ist. Wegen $\mathrm{Rg}_K(X) = 2 \leq \mathrm{Rg}_K(Y)$ folgt $Y = X^\eta$. Hieraus folgt dann $H_1^\gamma = H_1$ im Widerspruch zu (2). Also ist doch $\mathrm{Rg}_K(V) = 3$.

Weil der Rang von V endlich ist, ist der zu $L_K(V)$ duale Verband nach I.5.7 ebenfalls ein projektiver Verband. Wir dürfen daher annehmen, dass es ein $\eta \in G$ gibt mit $Y^\eta \neq Y$. Nach (4) ist dann $Y^\eta \leq X$, da Y^η ein von Y verschiedener Fixpunkt von γ ist. Weil C_1 kein Fixpunkt von γ ist, ist $Y^\eta \neq C_1$. Weil X eine Fixgerade von γ ist, H_1 aber nicht, ist X^η auch von $X \cup H_1$ verschieden. Folglich gilt auch $Y^\eta \neq Y^{\eta\sigma}$. Damit haben wir in $Y^{\eta\sigma}$ einen dritten Fixpunkt von γ gefunden.

Es sei $X^G = X$. Dann ist $Y \leq X$, da ja $Y^\eta \leq X$ ist. Hieraus folgt $A = X$ und mit (1) dann $B = \{0\}$. Es gibt daher ein $\delta \in G$ mit $Y \not\leq H_\delta$. Nun ist

$$Y = Y \cup X \leq H_1 \cup X < X.$$

Daher ist $Y = H_1 \cup X$. Setzt man $Z := H_1 \cup H_\delta$, so ist also $Z \neq Y$ und folglich $Z \not\leq X$. Ersetzt man in unserer bisherigen Argumentation γ durch δ, so sieht man, dass $A = Z + C_1$ ist. Hiermit folgt der Widerspruch $Z \leq A = X$. Also ist X keine Fixgerade von G.

Da X keine Fixgerade von G ist, hat γ nur die drei Fixpunkte Y, Y^η und $Y^{\eta\sigma}$. Diese Fixpunkte sind überdies nicht kollinear. Ferner gilt

$$Y^{\eta\sigma\eta} = Y^{\sigma\eta^{-1}\eta} = Y.$$

Hieraus folgt, dass $Y^{\eta^2} = Y^{\eta\sigma}$ ist, so dass die Fixpunkte von γ von der von η erzeugten Gruppe transitiv permutiert werden. Alles, was wir von γ sagten, gilt aber auch für η, so dass auch η genau drei Fixpunkte hat. Diese sind von den Fixpunkten von γ verschieden. Es bezeichne S die Menge der Kollineationen aus G, die die Fixpunkte von γ einzeln festlassen. Die Gruppe S lässt die Menge der Fixpunkte von η invariant. Da γ zu S gehört, operiert S auf der Menge der Fixpunkte von η transitiv. Weil die von 1 verschiedenen Elemente aus G aber alle nur drei Fixpunkte haben, folgt, dass S die Ordnung 3 hat. Dies wiederum hat zur Folge, dass G die Ordnung 9 hat.

Weil G die Ordnung 9 hat, enthält GZ genau 9 involutorische Streckungen. Sind nun γ, $\delta \in G$, so ist $C_\gamma^{\delta\sigma}$ ein von C_γ und C_δ verschiedenes Zentrum einer

involutorischen Streckung aus GZ auf $C_\gamma + C_\delta$. Beachte man, dass $\sigma\xi\sigma = \xi^{-1} = \xi^2$ ist für alle $\xi \in G$, so folgt

$$(\delta\sigma)^{-1}\gamma\sigma\delta\sigma = (\gamma\delta)^2\sigma.$$

Hieraus folgt $C_\gamma^{\delta\sigma} = C_{(\gamma\delta)^2}$, so dass die Zentren C_γ, C_δ und $C_{(\gamma\delta)^2}$ stets kollinear sind. Dieses Tripel ist eine Bahn der von $\gamma\delta^{-1}$ erzeugten Untergruppe von G. Denn es ist ja, wie wir früher gesehen haben, $C_\xi^\eta = C_{\eta^{-2}\xi} = C_{\eta\xi}$. Nun haben wir aber gezeigt, dass $A = V$ ist. Somit sind nicht alle C_ξ kollinear. Mit den zuvor gemachten Bemerkungen folgt dann, dass jede Gerade von $L_K(V)$, die zwei der Zentren trägt, genau drei von ihnen trägt. Hieraus folgt dann aber mühelos, dass die C_ξ's die Punkte einer affinen Unterebene von $L_K(V)$ sind.

Dass die letzte Situation tatsächlich vorkommt, haben wir im letzten Abschnitt gesehen.

8.3. Satz. *Es sei V ein Vektorraum über dem Körper K, dessen Rang mindestens 3 sei. Ferner seien P ein Punkt, H eine Hyperebene sowie U und W Unterräume von $L_K(V)$ und es gelte $V = P \oplus H = U \oplus W$. Ist σ eine Involution aus $\Lambda(U, W)$ und gilt $P^\sigma = P$ sowie $H^\sigma = H$, so ist σ mit allen Streckungen aus $\Delta(P, H)$ vertauschbar.*

Beweis. Weil P ein Fixpunkt von σ ist, ist $P \leq U$ oder $P \leq W$. Wir dürfen annehmen, dass $P \leq U$ ist. Wir dürfen ferner annehmen, dass $u\sigma = -u$ ist für alle $u \in U$ und dass $w^\sigma = w$ ist für alle $w \in W$. Wegen $H^\sigma = H$ ist

$$H = (H \cup U) \oplus (H \cup W).$$

Wegen $P \leq U$ folgt

$$V = P + H = U + (H \cup U) + (H \cup W) = U + (H \cup W).$$

Hieraus erhalten wir mit Hilfe des Modulargesetzes

$$W = W \cup V = W \cup \big(U + (H \cup W)\big) = H \cup W.$$

Somit ist $W \leq H$. Ist nun $\lambda \in \Delta(P, H)$, so ist also $U^\lambda = U$ und $W^\lambda = W$. Somit ist $\lambda^{-1}\sigma\lambda$ eine Involution aus $\Lambda(U, W)$. Da diese Gruppe aber nur eine Involution enthält, folgt $\lambda^{-1}\sigma\lambda = \sigma$, womit der Satz bewiesen ist.

8.4. Satz. *Es seien K und L Körper der Charakteristik $p > 0$. Ferner sei X ein Vektorraum über L des Ranges mindestens 2. Ist dann $K^*/Z(K^*)$ zu $\mathrm{PG^*L}(X, L)$ isomorph, so ist $\mathrm{Rg}_L(X) = 2$ und L ist kommutativ.*

Beweis. Wir beginnen den Beweis mit einer Vorbemerkung. Es sei X ein Vektorraum des Ranges 2 über L. Ist x_1, x_2 eine Basis von X und definiert man τ durch $x_1^\tau := x_1$ und $x_2^\tau := x_1 + x_2$, so ist die Ordnung von τ gleich p. Ist γ definiert durch $x_1^\gamma := x_1 a + x_2 c$ und $x_2^\gamma := x_1 b + x_2 d$ und ist $v^{\tau\gamma} = v^{\gamma\tau}$ für alle $v \in X$, so gelten die Gleichungen

$$\begin{aligned} a &= (a + c)r, \\ c &= cr, \\ a + b &= (b + d)r, \\ d &= dr. \end{aligned}$$

Da c und d nicht beide gleich Null sein können, ist $r = 1$. Dann ist aber $c = 0$ und $d = a$, so dass also $x_1^\gamma = x_1 a$ und $x_2^\gamma = x_1 b + x_2 a$ ist.

Sind umgekehrt $a, b \in L$, ist $a \neq 0$ und definiert man die Abbildung γ durch $x_1^\gamma := x_1 a$ und $x_2^\gamma := x_1 b + x_2 a$, so ist $\tau\gamma = \gamma\tau$. Ist nun H der Zentralisator von τ in $\mathrm{PGL}(X, L)$ und ist H_2 diejenige Untergruppe von H, die von allen γ der Form $x_1^\gamma = x_1$ und $x_2^\gamma = x_1 b + x_2$ induziert wird, so ist H_2 ein abelscher p-Normalteiler von H und H/H_2 ist isomorph zu $L^*/Z(L^*)$. Ferner folgt, wie eine einfache Rechnung zeigt, dass L genau dann kommutativ ist, wenn $H_2 \subseteq Z(H)$ gilt.

Es sei nun $kZ(K^*)$ ein Element der Ordnung p aus $K^*/Z(K^*)$. Ferner sei $x \in K^*$ und es gelte $x^{-1}kZ(K^*)x = kZ(K^*)$. Dann gibt es ein $z \in Z(K^*)$ mit $x^{-1}kx = kz$. Wegen $k^p \in Z(K^*)$ gilt daher

$$k^p = x^{-1}k^p x = k^p z^p,$$

so dass $z = 1$ ist. Der Zentralisator C von $kZ(K^*)$ in $K^*/Z(K^*)$ wird also durch den Zentralisator F^* von k in K^* induziert. Dann ist aber $F := F^* \cup \{0\}$ ein Teilkörper von K.

Es sei φ ein Isomorphismus von $\mathrm{PG^*L}(X, L)$ auf $K^*/Z(K^*)$. Ferner sei τ eine von 1 verschiedene Elation aus $\mathrm{PG^*L}(X, L)$ und H sei der Zentralisator von τ in $\mathrm{PG^*L}(X, L)$. Mit H_2 bezeichnen wir die Gruppe aller Elationen, deren Achse gleich der Achse von τ ist. Dann ist H_2 ein abelscher p-Normalteiler von H. Ferner sei S definiert durch $S/Z(K*) = H_2^\varphi$. Dann ist $S/Z(K^*)$ ein abelscher p-Normalteiler von $F^*/Z(K^*)$, wobei F wie im Absatz zuvor bestimmt sei, wobei hier $\varphi(\tau)$ die Rolle von k spielt. Es ist dann $H^\varphi = F^*/Z(K^*)$. Ferner ist klar, dass $Z(K^*) \subseteq Z(F^*)$ ist. Weil F ein Körper ist, folgt mit 5.9 b), dass $S \subseteq Z(F^*)$ ist. Somit ist $H_2^\varphi \subseteq Z(H)$. Mittels 5.10 folgt, dass der Rang von X nicht größer als 2 sein kann, so dass $\mathrm{Rg}_L(X) = 2$ ist. Aus unserer Vorbemerkung folgt dann weiter, dass L kommutativ ist, da ja H_2 hier wie dort die gleiche Bedeutung hat.

Nun haben wir alle Vorbereitungen getroffen, um den Beweis des folgenden Satzes anzugehen, der jedoch immer noch eine ganze Weile in Anspruch nehmen wird.

8.5. Satz. *Es sei V ein Vektorraum über dem Körper K und W sei ein Vektorraum über dem Körper L. Beide Vektorräume haben mindestens den Rang* 3. *Ist φ ein Isomorphismus von* $\mathrm{PG^*L}(V)$ *auf* $\mathrm{PG^*L}(W)$, *so gibt es einen Isomorphismus oder einen Antiisomorphismus σ von $L_K(V)$ auf $L_L(W)$, so dass $\gamma^\varphi = \sigma^{-1}\gamma\sigma$ ist für alle $\gamma \in \mathrm{PG^*L}(V)$.*

Beweis. Wir zeigen zunächst, dass K genau dann die Charakteristik 2 hat, wenn L die Charakteristik 2 hat. Weil φ^{-1} ein Isomorphismus von $\mathrm{PG^*L}(W)$ auf $\mathrm{PG^*L}(V)$ ist, genügt es dazu zu zeigen, dass L die Charakteristik 2 hat, wenn K die Charakteristik 2 hat.

Es sei $\mathrm{Char}(K) = 2 \neq \mathrm{Char}(L)$. Ferner sei τ eine von 1 verschiedene Elation von $L_K(V)$. Mit H bezeichnen wir den Zentralisator von τ in $\mathrm{PG^*L}(V)$. Ferner sei

$$\{1\} \subseteq H_2 \subseteq H_1 \subseteq H_0 \subseteq H$$

die in 5.10 beschriebene Normalreihe von H. Setze $\sigma := \tau^\varphi$. Dann ist σ eine Involution aus $\mathrm{PG}^*\mathrm{L}(W)$, da τ wegen $\mathrm{Char}(K) = 2$ eine Involution ist. Ist C der Zentralisator von σ in $\mathrm{PG}^*\mathrm{L}(W)$, so ist $H^\varphi = C$.

Eine längere Argumentationskette wird zeigen, dass σ durch eine Involution aus $\mathrm{G}^*\mathrm{L}(W)$ induziert wird, was dann seinerseits auf einen Widerspruch führt. Wir nehmen daher zunächst an, σ werde nicht durch eine Involution aus $\mathrm{G}^*\mathrm{L}(W)$ induziert. Nach 6.2 und 6.5 enthält C dann einen Normalteiler N vom Index 2. Ferner ist nach diesen Sätzen $N/Z(N) \cong \mathrm{PG}^*\mathrm{L}(X, F)$, wobei F ein Körper mit $Z(L) \subseteq F$ ist. Operiert σ fixpunktfrei, so ist F eine quadratische Erweiterung von L, so dass also $|F| > 3$ ist. Ferner ist $\mathrm{Rg}_F(X) = \frac{1}{2}\mathrm{Rg}_L(W) \geq \frac{3}{2}$, so dass $\mathrm{Rg}_F(X) \geq 2$ ist. Hat σ einen Fixpunkt, so ist $\mathrm{Rg}_F(X) = \mathrm{Rg}_L(W) \geq 3$. Es ist also stets $\mathrm{Rg}_F(X) \geq 2$ und X ist nicht der Vektorraum vom Range 2 über $\mathrm{GF}(2)$ oder $\mathrm{GF}(3)$. Schließlich ist $Z(N) \cong Z(F^*)/Z(L^*)$ und $Z(C) = \{1, \sigma\}$.

Es sei M ein in H_1^φ enthaltener Normalteiler von C. Angenommen, es wäre $MZ(N) \cap N \neq Z(N)$. Dann enthielte $(MZ(N) \cap N)/Z(N)$ nach 2.8 eine zu $\mathrm{PSL}(X, F)$ isomorphe Untergruppe, da ja $\mathrm{Rg}_F(X) \geq 2$ und da X nicht der Vektorraum vom Range 2 über $\mathrm{GF}(2)$ oder $\mathrm{GF}(3)$ ist. Dies widerspricht aber der Tatsache, dass $\mathrm{PSL}(X, F)$ keine 2-Gruppe ist. Also ist $MZ(N) \cap N = Z(V)$. Hieraus folgt $M \cap N \subseteq Z(N)$. Daher ist entweder $M \subseteq Z(N)$ oder $MN = C$, da ja N ein Normalteiler vom Index 2 in C ist.

Weil τ eine Elation und weil $\mathrm{Rg}_K(V) \geq 3$ ist, ist H_1 nicht abelsch. Daher ist H_1^φ keine Untergruppe von $Z(N)$. Nach der gerade gemachten Bemerkung ist daher $C = H_1^\varphi N$.

Es sei $Z(H_1^\varphi) \subseteq Z(N)$. Wegen $C_H(Z(H_1^\varphi) = H_0^\varphi$ ist dann $N \subseteq H_0^\varphi$. Daher ist

$$H^\varphi = C = NH_1^\varphi \subseteq NH_0^\varphi = H_0^\varphi,$$

so dass $H = H_0$ ist. Mit 5.10 folgt hieraus, dass K kommutativ ist. Hieraus folgt ebenfalls mit 5.10, dass das Zentrum von H zur additiven Gruppe von K isomorph ist. Aus $|Z(C)| = 2$ folgt daher, dass $|K| = 2$ ist. Dies hat wiederum zur Folge, dass die Gruppen $\mathrm{G}^*\mathrm{L}(A/P)$ und $\mathrm{PG}^*\mathrm{L}(A/P)$ isomorph sind, wenn A die Achse und P das Zentrum von τ bezeichnen. Nun ist $\mathrm{PG}^*\mathrm{L}(X, F)$ nicht auflösbar, so dass C und damit H nicht auflösbar ist. Dann ist aber auch $\mathrm{PG}^*\mathrm{L}(A/P)$ nicht auflösbar. Aus 2.8 folgt daher, dass $\mathrm{PG}^*\mathrm{L}(A/P)$ und damit $H_0/H_1 = H/H_1$ keinen von $\{1\}$ verschiedenen abelschen Normalteiler enthält. Folglich ist

$$H_1 Z(N)^{\varphi^{-1}}/H_1 = \{1\},$$

so dass $Z(N)^{\varphi^{-1}} \subseteq H_1$ ist. Also ist $Z(N)$ eine abelsche 2-Gruppe vom Exponenten 2 oder 4. Nun ist $Z(N) \cong Z(F^*)/Z(L^*)$. Ist $f \in Z(F^*) - Z(L^*)$ und $f^2 \in Z(L^*)$, so ist, da der Exponent von $Z(N)$ ein Teiler von 4 ist,

$$1 + 4f + 6f^2 + 4f^3 + f^4 = (1 + f)^4 \in Z(L).$$

Weil die Charakteristik von L von 2 verschieden ist und wir angenommen haben, dass $f^2 \in Z(L)$ ist, folgt weiter

$$f(f^2 + 1) \in Z(L).$$

Weil f aber kein Element von $Z(L)$ ist, folgt $f^2 + 1 = 0$. Dies besagt, dass f eine primitive vierte Einheitswurzel von $Z(F)$ ist. Das impliziert wiederum, dass $Z(N)$ höchstens eine und damit genau eine Involution enthält. Da $Z(N)$ eine abelsche Gruppe vom Exponenten 2 oder 4 ist, folgt, dass $Z(N)$ eine zyklische Gruppe der Ordnung 2 oder 4 ist. Weil $Z(F)$ und $Z(L)$ Körper sind, ist $|Z(F^*)/Z(L^*)| > 2$, daher ist $Z(N)$ die zyklische Gruppe der Ordnung 4. Wegen $N \cap H_1^\varphi \subseteq Z(N)$ ist $N \cap H_1 = Z(N)$. Daher folgt aus

$$C/N = (NH_1^\varphi)/N \cong H_1^\varphi/(N \cap H_1^\varphi) = H_1^\varphi/Z(N),$$

dass $|H_1| = 2|Z(N)| = 8$ ist. Dies impliziert, dass V endlich ist.

Es sei n der Rang von V. Dann ist, da $\mathrm{Rg}_K(A) = n - 1$ und $\mathrm{Rg}_K(P) = 1$ sowie $|K| = 2$ ist,

$$\big|\mathrm{Hom}_K(A/P, P)\big| = 2^{n-2}$$

und

$$\big|\mathrm{Hom}_K(V/A, A)\big| = 2^{n-1}.$$

Mit 5.10 folgt hieraus

$$2^3 = |H_1/H_2| \cdot |H_2| = 2^{2n-3}$$

und damit $n = 3$. Dies impliziert $\mathrm{Rg}_K(A/P) = 1$, was wiederum $\mathrm{G^*L}(A/P) = \{1\}$ nach sich zieht, so dass H auflösbar ist. Dieser Widerspruch zeigt, dass $Z(H_1^\varphi)$ nicht in $Z(N)$ enthalten ist. Dann ist aber, wie wir gesehen haben, $NZ(H_1^\varphi) = C$. Ferner ist $N \cap Z(H_1^\varphi) \subseteq Z(N)$. Hieraus folgt

$$N \cap Z(H_1^\varphi) \subseteq Z(NH_1^\varphi) = Z(C).$$

Andererseits ist

$$Z(C) \subseteq N \cap Z(H_1^\varphi).$$

Also ist

$$\big|N \cap Z(H_1^\varphi)\big| = 2.$$

Aus $|C/N| = 2$ und $C = NZ(H_1^\varphi)$ folgt daher $|Z(H_1^\varphi)| = 4$. Nach 5.10 ist $Z(H_1)$ zu $\mathrm{Hom}_K(V/A, P)$ isomorph. Da hiernach $\mathrm{Hom}_K(V/A, P)$ genau vier Elemente enthält, hat auch K genau vier Elemente. Somit ist K kommutativ. Nach 5.10 ist daher $H = H_0$ und daher $Z(H) = Z(H_1)$. Hiermit folgt der Widerspruch

$$2 = \big|Z(H)\big| = \big|Z(H_0)\big| = 4.$$

Dieser Widerspruch rührt daher, dass wir annahmen, σ würde nicht durch eine Involution aus $\mathrm{G^*L}(W)$ induziert, so dass diese Annahme also zu verwerfen ist.

Die Kollineation σ wird also durch eine Involution induziert. Ist H auflösbar, so ist auch C auflösbar. Nach 6.6, 5.10 bzw. 5.4 und 2.6 folgt dann $|K| = 2$ und $|L| = 3$ sowie $\mathrm{Rg}_K(V) \leq 4$ und $\mathrm{Rg}_L(W) \leq 4$. Nach 1.7 und 1.13 ist aber

$$\begin{aligned}
\big|\mathrm{PG^*L}(3,2)\big| &= 2^3 \cdot 3 \cdot 7,\\
\big|\mathrm{PG^*L}(4,2)\big| &= 2^6 \cdot 3^2 \cdot 5 \cdot 7,\\
\big|\mathrm{PG^*L}(3,3)\big| &= 3^3 \cdot 2^4 \cdot 13,\\
\big|\mathrm{PG^*L}(4,3)\big| &= 3^6 \cdot 2^8 \cdot 5 \cdot 13,
\end{aligned}$$

so dass $\mathrm{PG^*L}(V)$ und $\mathrm{PG^*L}(W)$ nicht isomorph sein können. Also ist H und damit auch C nicht auflösbar.

Nach 6.6 gibt es Unterräume X und Y von W mit $W = X \oplus Y$ und $\sigma \in \Lambda(X,Y)$. Nach 5.2 ist $\Lambda(X,Y)$ zur multiplikativen Gruppe von L oder von $Z(L)$ isomorph. Weil σ involutorisch ist, liegt σ in jedem Falle im Zentrum von $\Lambda(X,Y)$. Es sei nun Λ_1 diejenige Untergruppe von $\mathrm{PG^*L}(W)$, die X als Ganzes und Y punktweise festlässt, und Λ_2 sei diejenige Untergruppe von $\mathrm{PG^*L}(W)$, die X punktweise und Y als Ganzes festlässt. Nach 5.5 ist dann

$$|C : \Lambda_1\Lambda_2| \leq 2.$$

Liegt H_1^φ nicht in $\Lambda_1\Lambda_2$, so ist $C \neq \Lambda_1\Lambda_2$ und daher $|C : \Lambda_1\Lambda_2| = 2$. Es folgt $C = \Lambda_1\Lambda_2 H_1^\varphi$. Dies impliziert seinerseits, dass es ein $\eta \in H_1^\varphi$ gibt mit $\eta^{-1}\Lambda_1\eta = \Lambda_2$. Aus $|C : \Lambda_1\Lambda_2| = 2$ und $C = \Lambda_1\Lambda_2 H_1^\varphi$ folgt, dass

$$\big|H_1^\varphi : \big((\Lambda_1\Lambda_2) \cap H_1^\varphi\big)\big| = 2$$

ist. Ferner ist $(\Lambda_1\Lambda_2) \cap H_1^\varphi$ ein 2-Normalteiler von $\Lambda_1\Lambda_2$. Hieraus folgt, dass

$$\big(\Lambda(X,Y)((\Lambda_1\Lambda_2) \cap H_1^\varphi)\big)/\Lambda(X,Y)$$

ein 2-Normalteiler von

$$(\Lambda_1\Lambda_2)/\Lambda(X,Y)$$

ist. Nach 5.4 e) ist $(\Lambda_1\Lambda_2)/\Lambda(X,Y)$ zu

$$\mathrm{PG^*L}(X) \times \mathrm{PG^*L}(Y)$$

isomorph. Weil $\eta^{-1}\Lambda_1\eta = \Lambda_2$ ist, ist $X^\eta = Y$, so dass $\mathrm{Rg}_L(X) = \mathrm{Rg}_L(Y) \geq 2$ ist. Enthielte $\Lambda_1\Lambda_2/\Lambda(X,Y)$ einen nicht trivialen 2-Normalteiler, so folgt $|L| = 3$ und $\mathrm{Rg}_L(X) = \mathrm{Rg}_L(Y) = 2$, so dass C und damit H auflösbar wäre. Dieser Widerspruch zeigt, dass

$$(\Lambda_1\Lambda_2) \cap H_1\varphi \subseteq \Lambda(X,Y)$$

gilt. Wegen $\mathrm{Rg}_L(X) = \mathrm{Rg}_L(Y) \geq 2$ ist $\Lambda(X,Y) \cong Z(K^*)$ nach 5.4 e). Weil der Exponent von H_1^φ gleich 4 ist, folgt daher

$$\big|(\Lambda_1\Lambda_2) \subseteq H_1^\varphi\big| \leq 4,$$

so dass $|H_1| = |H_1^\varphi| \leq 8$ ist. Folglich ist wieder $|K| = 2$ und $\mathrm{Rg}_K(V) = 3$, was den Widerspruch der Auflösbarkeit von H nach sich zieht. Also ist doch $H_1^\varphi \subseteq \Lambda_1\Lambda_2$.

Weil der Rang von V mindestens 3 ist, folgt mit 5.10, dass H_2 mindestens zwei Involutionen enthält. Daher kann H_2^φ nicht in der Gruppe $\Lambda(U,V)$ enthalten sein, da diese Gruppe zur multiplikativen Gruppe von L oder $Z(L)$ isomorph ist. Hieraus folgt, dass

$$\big(\Lambda(X,Y)H_1^\varphi\big)/\Lambda(X,Y)$$

ein nicht trivialer 2-Normalteiler von $(\Lambda_1\Lambda_2)/\Lambda(X,Y)$ ist. Nun ist

$$(\Lambda_1\Lambda_2)/\Lambda(X,Y) \cong \mathrm{PG^*L}(X) \times \mathrm{PG^*L}(Y).$$

Weil C nicht auflösbar ist, können $\mathrm{PG^*L}(X)$ und $\mathrm{PG^*L}(Y)$ nicht beide auflösbar sein, da sonst L nur drei Elemente enthielte und C dann doch auflösbar wäre. Daher kann nur eine der Gruppen $\mathrm{PG^*L}(X)$ und $\mathrm{PG^*L}(Y)$ einen nicht trivialen 2-Normalteiler enthalten. Wir dürfen daher annehmen, dass die Gruppe $\mathrm{PG^*L}(X)$ einen zu $(\Lambda(X,Y)H_1^\varphi)/H_1^\varphi)/\Lambda(X,Y)$ isomorphen 2-Normalteiler enthält. Hieraus folgt $\mathrm{Rg}_L(X) = 1$ oder $|L| = 3$ und $\mathrm{Rg}_L(X) = 2$. Weil $\mathrm{PG^*L}(X)$ nicht trivial ist, kann aber der Fall $\mathrm{Rg}_L(X) = 1$ nicht eintreten. Dies impliziert, dass der maximale 2-Normalteiler der Gruppe $(\Lambda_1\Lambda_2)/\Lambda(X,Y)$ die Ordnung 4 hat. Weil $\Lambda(X,Y)$ zur multiplikativen Gruppe von K isomorph ist und folglich die Ordnung 3 hat, hat der maximale 2-Normalteiler von $\Lambda_1\Lambda_2$ die Ordnung 8. Hieraus folgt, dass $|H_1| = 8$ und $\mathrm{Rg}_K(V) = 3$ ist, was wiederum die Auflösbarkeit von H impliziert. Dieser Widerspruch zeigt endlich, dass die Charakteristik von L doch gleich 2 ist.

Es sei weiter$\mathrm{Char}(K) = 2$. Dann ist, wie wir jetzt wissen, auch $\mathrm{Char}(L) = 2$. Wir zeigen nun, dass jede Elation aus $\mathrm{PG^*L}(V)$ auf eine Elation aus $\mathrm{PG^*L}(W)$ abgebildet wird. Es sei also τ eine von eins verschiedene Elation aus $\mathrm{PG^*L}(V)$. Dann ist $\sigma := \tau^\varphi$ eine Involution aus $\mathrm{PG^*L}(W)$. Es sei wieder H der Zentralisator von τ in $\mathrm{PG^*L}(V)$ und C der Zentralisator von σ in $\mathrm{PG^*L}(W)$.

Wird σ nicht durch eine Involution aus $\mathrm{G^*L}(W)$ induziert, so ist die Faktorgruppe $C/Z(C)$ nach 6.2 bzw. 6.5 isomorph zur Gruppe $\mathrm{PG^*L}(X,F)$, wobei F ein Körper mit $Z(L) \subseteq F$ ist. Operiert σ fixpunktfrei auf $L_L(W)$, so ist F eine quadratische Erweiterung von L, so dass $|F| > 3$ ist. Ferner ist in diesem Falle $\mathrm{Rg}_F(X) = \frac{1}{2}\mathrm{Rg}_L(W) \geq 2$. Hat σ einen Fixpunkt, so ist $\mathrm{Rg}_F(X) = \mathrm{Rg}_L(W) \geq 3$. Es ist also stets $\mathrm{Rg}_F(X) \geq 2$ und X ist nicht der Vektorraum vom Range 2 über $\mathrm{GF}(2)$ bzw. $\mathrm{GF}(3)$. Mit Hilfe von 2.8 folgt daher, dass $C/Z(C)$ keinen von eins verschiedenen 2-Normalteiler enthält. Hieraus folgt, dass $H_1^\varphi \subseteq Z(C)$ ist. Dies widerspricht aber der Tatsache, dass H_1 nicht abelsch ist. Dieser Widerspruch zeigt, dass σ eine Quasielation ist.

Weil σ eine Quasielation ist, besitzt C eine Normalreihe $\{1\} \subseteq C_1 \subseteq C_0 \subseteq C$, wobei C der größte auflösbare 2-Normalteiler von C und C_0 der Zentralisator von $Z(C_1)$ in C ist. Daher ist $H_1^\varphi = C_1$ und $H_0^\varphi = C_0$. Hieraus folgt, dass H/H_0 zu C/C_0 isomorph ist. Ist K kommutativ, so ist $H = H_0$ und damit $C = C_0$. Dies besagt, dass σ eine Elation ist und dass auch L kommutativ ist. Ist σ keine Elation, so ist also K nicht kommutativ. Weil φ^{-1} ein Isomorphismus von $\mathrm{PG^*L}(W)$ auf $\mathrm{PG^*L}(V)$ ist, folgt, dass auch L nicht kommutativ ist. Ist nun B die Achse von σ, so ist $\mathrm{Rg}_L(W/B) \geq 2$. Ferner ist C/C_0 zu $\mathrm{PG^*L}(W/B)$ isomorph, so dass wegen $H/H_0 \cong K^*/Z(K^*)$ die Gruppen $K^*/Z(K^*)$ und $\mathrm{PG^*L}(W/B)$ isomorph sind. Wegen $\mathrm{Char}(K) = 2 = \mathrm{Char}(L)$ folgt daher mit 8.4 der Widerspruch, dass L kommutativ ist. Damit ist gezeigt, dass im Falle $\mathrm{Char}(K) = 2$ der Isomorphismus φ Elationen auf Elationen abbildet.

Es sei nun $\mathrm{Char}(K) \neq 2$. Wir wollen zeigen, dass φ auch in diesem Falle Elationen auf Elationen abbildet. Dazu zeigen wir zunächst, dass φ involutorische

Streckungen auf involutorische Streckungen abbildet. Zunächst notieren wir, dass auch die Charakteristik von L von 2 verschieden ist, wie wir nicht ohne Mühe zeigten. Es sei nun ρ eine involutorische Streckung von $L_K(V)$ mit der Achse A und dem Zentrum P. Es sei C der Zentralisator von ρ in $\mathrm{PG}^*\mathrm{L}(V)$. Es sei Λ_1 die Gruppe, die P punktweise und A als Ganzes festlässt, und Λ_2 sei die Gruppe, die A punktweise und P als Ganzes festlässt. Wegen $\mathrm{Rg}_K(P) = 1$ ist dann $\Lambda_2 = \Delta(P, A)$. Ferner ist $\Lambda_2 \subseteq \Lambda_1$, so dass insbesondere $\Lambda_1 = \Lambda_1\Lambda_2$ ist. Mit 5.4 folgt weiter, dass $|C : \Lambda_1| = 1$ oder 2 ist. Wegen $\mathrm{Rg}_K(P) = 1 < \mathrm{Rg}_K(A)$ kann der zweite Fall nach 5.4 nicht eintreten. Also ist $C = \Lambda_1$. Nochmals 5.4 zitierend sehen wir, dass $Z(C) = Z(\Delta(P, A))$ ist.

Wir setzen $\sigma := \rho^\varphi$ und bezeichnen mit D den Zentralisator von σ in $\mathrm{PG}^*\mathrm{L}(W)$. Wird σ nicht durch eine Involution aus $\mathrm{G}^*\mathrm{L}(W)$ induziert, so enthält D nach 6.2 bzw. 6.5 einen Normalteiler N vom Index 2 mit $N/Z(N) \cong \mathrm{PG}^*\mathrm{L}(X, F)$, wobei F ein Körper mit $Z(L) \subseteq F$ ist. Ferner ist, wie wir schon zweimal bemerkten, $\mathrm{Rg}_F(X) \geq 2$ und X ist nicht der Vektorraum vom Range 2 über GF(2) oder GF(3). Schließlich ist $Z(N) \cong Z(F^*)/Z(L^*)$ und $Z(D) = \{1, \sigma\}$. Wäre $|K| = 3$ und $\mathrm{Rg}_K(A) = 2$, so wäre C und damit D auflösbar, was nicht der Fall ist. Somit enthält $\Lambda_1/\Delta(P, A)$ wegen 2.8 keinen abelschen Normalteiler ungleich Eins. Hieraus folgt, dass $Z(N)^{\varphi^{-1}} \subseteq \Delta(P, A)$ ist. Wegen

$$Z(C) = Z(D)^{\varphi^{-1}} \subseteq Z(N)^{\varphi^{-1}}$$

enthält die multiplikative Gruppe von K einen abelschen Normalteiler A ungleich eins mit $Z(K^*) \subseteq A$. Da A einen kommutativen, normalen Teilkörper von K erzeugt, folgt nach dem Satz von Cartan-Brauer-Hua, dass $A \subseteq Z(K^*)$ ist. Also ist $A = Z(K^*)$ und daher $Z(C) = Z(N)^{\varphi^{-1}}$. Hieraus folgt $Z(N) = Z(D)$. Dies ergibt den Widerspruch $|Z(F^*)/Z(L^*)| = 2$. Somit ist σ eine Quasistreckung.

Angenommen σ ist keine Streckung. Ist $\mathrm{Rg}_K(A) = 2$ und $|K| = 3$, so ist $\mathrm{Rg}_K(V) = 3$ und C ist auflösbar. Dann ist auch D auflösbar, so dass nach 5.4 auch $|L| = 3$ sowie $\mathrm{Rg}_L(W) \leq 4$ ist. Ein Vergleich der Ordnungen von $\mathrm{PG}^*\mathrm{L}(V)$ und $\mathrm{PG}^*\mathrm{L}(W)$ zeigt, dass auch der Rang von W gleich 3 ist. Dann ist σ aber eine Streckung. Also ist V nicht der Vektorraum vom Range 3 über GF(3).

Es sei $W = X \oplus Y$ und $\sigma \in \Lambda(X, Y)$. Ferner sei Q ein Punkt in X und B ein Y umfassendes Komplement von Q. Ist λ die involutorische Streckung aus $\Delta(Q, B)$, so ist $X^\lambda = Y$ und $Y^\lambda = Y$. Daher ist $\lambda\sigma = \sigma\lambda$. Folglich ist $\lambda^{\varphi^{-1}}\rho = \rho\lambda^{\varphi^{-1}}$. Hieraus folgt, dass φ^{-1} sowohl P als auch A festlässt. Nach dem bereits Bewiesenen ist $\lambda^{\varphi^{-1}}$ eine involutorische Quasistreckung. Nach 8.3 wird folglich $\Delta(P, A)$ von $\lambda^{\varphi^{-1}}$ zentralisiert. Daher wird λ von $\Delta(P, A)^\varphi$ zentralisiert, woraus folgt, dass Q ein Fixpunkt von $\Delta(P, A)^\varphi$ ist. Weil Q ein beliebiger Punkt in X war, heißt das, dass X von $\Delta(P, A)^\varphi$ punktweise festgelassen wird. Ebenso zeigt man, dass $\Delta(P, A)^\varphi$ auch Y punktweise festlässt. Somit ist $\Delta(P, A)^\varphi$ eine Untergruppe von $\Lambda(X, Y)$. Weil σ keine Streckung ist, ist $\Lambda(X, Y)$ nach 5.2 b) abelsch. Folglich ist $\Delta(P, A)$ abelsch, so dass nach 5.4 f) die Gleichung $Z(C) = \Delta(P, A)$ gilt. Weil $C/\Delta(P, A)$ nicht auflösbar ist, folgt aus 2.8, dass $C/\Delta(P, A)$ keinen nicht trivialen abelschen Normalteiler enthält.

Da andererseits $\Lambda(X,Y)^{\varphi^{-1}}/\Delta(P,A)$ ein abelscher Normalteiler dieser Gruppe ist, folgt $\Lambda(X,Y)^{\varphi^{-1}} = \Delta(P,A)$. Hieraus folgt, dass φ^{-1} einen Isomorphismus von $D/\Lambda(X,Y)$ auf $C/\Delta(P,A)$ induziert. Daher enthält die Gruppe $\mathrm{PG^*L}(A)$ einen Normalteiler $N = N_1 \times N_2$ mit $N_1 \cong \mathrm{PG^*L}(X)$ und $N_2 \cong \mathrm{PG^*L}(Y)$. Aus 2.8 folgt wiederum, dass $\mathrm{PSL}(A)$ in N enthalten ist, so dass sowohl N_1 als auch N_2 die Gruppe $\mathrm{PSL}(A)$ normalisieren. Eine nochmalige Anwendung von 2.8 liefert daher den Widerspruch $\mathrm{PSL}(A) \subseteq N_1 \cap N_2 = \{1\}$. Dieser Widerspruch zeigt, dass σ doch eine involutorische Streckung ist.

Wir zeigen nun, dass φ auch im Falle einer von 2 verschiedenen Charakteristik die Elationen aus $\mathrm{PG^*L}(V)$ auf die Elationen von $\mathrm{PG^*L}(W)$ abbildet. Um dies zu zeigen, sei H — der Buchstabe H steht wieder zur Verfügung — eine Hyperebene von $L_K(V)$ und G sei die Gruppe aller Elationen mit der Achse H. Schließlich sei σ eine involutorische Streckung mit der Achse H und Z sei die von σ erzeugte Gruppe der Ordnung 2. Nach 8.1 ist die Gruppe G ihr eigener Zentralisator in $\mathrm{PG^*L}(V)$ und weil die Charakteristik von K von 2 verschieden ist, enthält G auch keine Involution. Ferner ist $|GZ : G| = 2$, so dass die Kollineationen $\gamma\sigma$ mit $\gamma \in G$ involutorische Streckungen mit der Achse H sind. Weil G auf der Punktmenge von $L_K(V)_H$ transitiv operiert, gibt es zu jedem $\gamma \in G$ ein $\eta \in G$ mit $\gamma\sigma = \eta^{-1}\sigma\eta$. Folglich erfüllen G und σ die Voraussetzungen von 8.2. Nun ist σ^φ eine involutorische Streckung von $L_L(W)$, wie wir gesehen haben. Daher erfüllen auch G^φ und σ^φ die Voraussetzungen von 8.2. Somit ist G^φ eine Gruppe von Elationen, es sei denn, es ist $\mathrm{Rg}_L(W) = 3$ und G hat die Ordnung 9. In diesem Falle besitzt $L_K(V)_H$ aber nur neun Punkte, so dass V der Vektorraum vom Rang 3 über $\mathrm{GF}(3)$ ist. Weil die Gruppen $\mathrm{PG^*L}(V)$ und $\mathrm{PG^*L}(W)$ isomorph sind, folgt dann, dass auch $L = \mathrm{GF}(3)$ ist. Weil die Zentren der Streckungen aus $(GZ)^\varphi$ die Punkte einer affinen Unterebene der Ordnung 3 von $L_L(W)$ ist, folgt mittels 7.2 und 7.6, dass die Streckungen aus $(GZ)^\varphi$ doch alle die gleiche Achse haben. Also kann dieser Fall nicht eintreten. Dies zeigt, dass φ Elationen auf Elationen abbildet.

Es sei nun P ein Punkt und H eine Hyperebene von $L_K(V)$. Offensichtlich gilt genau dann $P \leq H$, wenn $\mathrm{E}(P) \cap \mathrm{E}(H) \neq \{1\}$ ist. Weil φ Elationen auf Elationen abbildet, sind $\mathrm{E}(P)^\varphi$ und $\mathrm{E}(H)^\varphi$ Gruppen von Elationen. Mit 8.1 folgt die Existenz von Unterräumen P^ρ bzw. H^ρ von W mit $\mathrm{Rg}_L(P^\rho) = 1$ bzw. $\mathrm{KoRg}_L(P^\rho) = 1$ und $\mathrm{KoRg}_L(H^\rho) = 1$ bzw. $\mathrm{Rg}_L(H^\rho) = 1$, so dass $\mathrm{E}(P)^\varphi = \mathrm{E}(P^\rho)$ und $\mathrm{E}(H)^\varphi = \mathrm{E}(H^\rho)$ ist. Nun sind $\mathrm{E}(P)$ und $\mathrm{E}(H)$ nicht konjugiert unter $\mathrm{PG^*L}(V)$, so dass $\mathrm{E}(P^\rho)$ und $\mathrm{E}(H^\rho)$ in verschiedenen Konjugiertenklassen von $\mathrm{PG^*L}(W)$ liegen. Daher ist entweder

$$\mathrm{Rg}_L(P^\rho) = \mathrm{KoRg}_L(H^\rho) = 1$$

für alle Punkte P und alle Hyperebenen H von $L_K(V)$ oder es ist

$$\mathrm{KoRg}_L(P^\rho) = \mathrm{Rg}_L(H^\rho) = 1$$

für alle Punkte P und alle Hyperebenen H von $L_K(V)$. In beiden Fällen ist ρ eine Bijektion der Menge der Punkte und der Hyperebenen von $L_K(V)$ auf die Menge der Punkte und Hyperebenen von $L_L(V)$. Im ersten Falle werden dabei

die Punktmenge auf die Punktmenge und die Hyperebenenmenge auf die Hyperebenenmenge abgebildet, während im zweiten Falle die Punktmenge auf die Hyperebenenmenge und die Hyperebenenmenge auf die Punktmenge abgebildet werden. Weil genau dann $\mathrm{E}(P) \cap \mathrm{E}(H) \neq \{1\}$ gilt, wenn $\mathrm{E}(P^\rho) \cap \mathrm{E}(H^\rho) \neq \{1\}$ gilt, ist ρ in beiden Fällen inzidenztreu. Mit I.8.6 und der Übungsaufgabe zu diesem Satz folgt, dass ρ durch einen Isomorphismus oder Antiisomorphismus σ von $L_K(V)$ auf $L_L(W)$ induziert wird.

Es sei schließlich $\gamma \in \mathrm{PG^*L}(V)$. Dann ist

$$\mathrm{E}(P^{\sigma\gamma^\varphi}) = \gamma^{-\varphi}\mathrm{E}(P^\sigma)\gamma^\varphi = \gamma^{-1}\mathrm{E}(P)^\varphi\gamma^\varphi = (\gamma^{-1}\mathrm{E}(P)\gamma)^\varphi = \mathrm{E}(P^\gamma)^\varphi = \mathrm{E}(P^{\gamma\sigma}).$$

Hieraus folgt $P^{\sigma\gamma^\varphi} = P^{\gamma\sigma}$ für alle Punkte P von $L_K(V)$. Da ein Isomorphismus bzw. ein Antiisomorphismus durch seine Wirkung auf die Punkte bereits festgelegt wird, folgt $\sigma\gamma^\varphi = \gamma\sigma$, so dass

$$\gamma^\varphi = \sigma^{-1}\gamma\sigma$$

für alle $\gamma \in \mathrm{PG^*L}(V)$ gilt. Damit ist 8.5 endlich bewiesen.

Das folgende Korollar ist eine unmittelbare Folgerung aus 8.5.

8.6. Korollar. *Sei V ein Vektorraum über dem Körper K mit* $\mathrm{Rg}_K(V) \geq 3$.

a) *Ist $L_K(V)$ nicht selbstdual, so ist* $\mathrm{P\Gamma L}(V)$ *zur Automorphismengruppe von* $\mathrm{PG^*L}(V)$ *isomorph.*
b) *Ist $L_K(V)$ selbstdual, so enthält die Automorphismengruppe von* $\mathrm{PG^*L}(V)$ *einen zu* $\mathrm{P\Gamma L}(V)$ *isomorphen Normalteiler vom Index* 2.
c) *Die Gruppen* $\mathrm{PSL}(V)$ *und $PGL(V)$ sind charakteristische Untergruppen von* $\mathrm{PG^*L}(V)$*, dh., sie sind unter allen Automorphismen von* $\mathrm{PG^*L}(V)$ *invariant.*

Der Leser wird vielleicht fragen, wie man auf all dies komme. Diese Frage kann ich hier ausnahmsweise einmal beantworten. Geometrisch sind Elationen und Streckungen am besten zu fassen, gruppentheoretisch Involutionen. Daher stellt man zuerst die Frage, wie man die unterschiedlichen Involutionen in den fraglichen Gruppen unterscheiden kann. Da drängen sich ihre Zentralisatoren auf. Der Rest ist eine genaue Analyse der Situation gepaart mit Routine. Dann entgeht einem auch die hessesche Gruppe nicht, die ich nirgends in der Literatur in der vorliegenden Allgemeinheit behandelt fand.

IIII.

Endliche projektive Geometrien

In diesem Kapitel studieren wir zunächst kombinatorische Eigenschaften endlicher projektiver Geometrien. Wir werden herausfinden, dass jede Kollineation einer projektiven Geometrie ebenso viele Fixpunkte wie Fixhyperebenen hat und dass die Anzahl der Punktbahnen einer Kollineationsgruppe gleich der Anzahl ihrer Hyperebenenbahnen ist. Wir werden auch sehen, dass es keine endlichen elliptischen Geometrien gibt, da Polaritäten endlicher projektiver Räume stets absolute Punkte haben. Später werden wir verschiedene Kennzeichnungen der endlichen, desarguesschen projektiven Ebenen innerhalb aller endlichen projektiven Ebenen geben. Diese Kennzeichnungen bedienen sich der Kollineationsgruppen dieser Ebenen. Außerdem geben wir noch verschiedene kombinatorische und gruppentheoretische Kennzeichnungen der endlichen projektiven Räume innerhalb der Klasse der projektiven Blockpläne.

Dieses Kapitel sieht beim ersten Hinschauen aus wie ein Sammelsurium der unterschiedlichsten Sätze. Dem aufmerksamen Leser wird aber nicht entgehen, dass ihm eine Kohärenz innewohnt, die sich bis zu dem Satz 11.3 von N. Ito erstreckt, dass also nichts in diesem Kapitel überflüssig ist.

1. Endliche Inzidenzstrukturen

Es sei Π eine Menge, deren Elemente wir Punkte, und B eine Menge, deren Elemente wir Blöcke nennen. Ferner sei $\mathrm{I} \subseteq \Pi \times \mathrm{B}$. Das Tripel $T := (\Pi, \mathrm{B}, \mathrm{I})$ heißt *Inzidenzstruktur* (siehe Kapitel I, Abschnitt 1). Die Elemente von I nennen wir *Fahnen* von T. Die Inzidenzstruktur $(\Pi, \mathrm{B}, \mathrm{I})$ heißt *endlich*, falls Π und B endlich sind.

Ist $T := (\Pi, \mathrm{B}, \mathrm{I})$ eine Inzidenzstruktur, so definieren wir die Inzidenzstruktur $T^d := (\Pi^d, \mathrm{B}^d, \mathrm{I}^d)$ durch $\Pi^d := \mathrm{B}$, $\mathrm{B}^d := \Pi$ und $\mathrm{I}^d := \{(b, P) \mid (P, b) \in \mathrm{I}\}$. Die Inzidenzstruktur T^d heißt die zu T *duale Inzidenzstruktur*. Offenbar ist $T^{dd} = T$.

Ist $(\Pi, \mathrm{B}, \mathrm{I})$ eine Inzidenzstruktur, so definieren wir auf I zwei Äquivalenzrelationen $\sim$ und $\approx$ durch $(P, b) \sim (Q, c)$ genau dann, wenn $P = Q$, bzw. $(P, b) \approx (Q, c)$ genau dann, wenn $b = c$ ist. Für $P \in \Pi$ bezeichne I_P die durch P bestimmte Äquivalenzklasse von $\sim$ und für $b \in \mathrm{B}$ bezeichne I_b die durch b bestimmte Äquivalenzklasse von $\approx$. Es gilt dann

$$\mathrm{I} = \bigcup_{P \in \Pi} \mathrm{I}_P = \bigcup_{b \in B} \mathrm{I}_b$$

und $I_P \cap I_Q = \emptyset$, falls $P \neq Q$, und $\mathrm{I}_b \cap \mathrm{I}_c = \emptyset$, falls $b \neq c$ ist. Ist r_P die Anzahl der Elemente in I_P, dh. die Anzahl der Blöcke, die mit P inzidieren, und ist k_b die Anzahl der mit b inzidierenden Punkte, so gilt also der folgende Satz.

1.1. Satz. *Ist* $(\Pi, \mathrm{B}, \mathrm{I})$ *eine endliche Inzidenzstruktur, so ist*

$$\sum_{P \in \Pi} r_P = |\,\mathrm{I}\,| = \sum_{b \in \mathrm{B}} k_b.$$

Die Inzidenzstruktur $T := (\Pi, \mathrm{B}, \mathrm{I})$ heißt *linksseitige taktische Konfiguration*, falls es eine ganze Zahl r gibt mit $r_P = r$ für alle $P \in \Pi$, und sie heißt *rechtsseitige taktische Konfiguration*, falls es eine ganze Zahl k gibt mit $k_b = k$ für alle $b \in \mathrm{B}$. Schließlich heißt T *taktische Konfiguration*, falls T sowohl linksseitige als auch rechtsseitige taktische Konfiguration ist.

Ist $T := (\Pi, \mathrm{B}, \mathrm{I})$ eine endliche Inzidenzstruktur, so setzen wir $v := |\Pi|$ und $b := |\mathrm{B}|$. Damit dürfen wir den Buchstaben b nicht mehr als Namen für einen Block verwenden. Die Anzahl der Blöcke b zu nennen, versteht sich von selbst. Die Anzahl der Punkte v zu nennen, rührt aus der Statistik, wo man endliche Inzidenzstrukturen beim Planen von Versuchen benutzt und v dann für das englische *variety* steht. Der Buchstabe r als Anzahl der Blöcke durch einen Punkt steht für *replication*. Ist T linksseitige taktische Konfiguration, so heißen v, r, k_c mit $c \in B$ Parameter von T, und ist T rechtsseitig taktische Konfiguration, so werden die Zahlen b, k, r_p mit $P \in \Pi$ Parameter von T genannt. Ist T taktische Konfiguration, so heißen v, b, k, r Parameter von T. Mit diesen Definitionen folgt aus 1.1 unmittelbar

1.2. Korollar. *Es sei* $T := (\Pi, \mathrm{B}, \mathrm{I})$ *eine endliche Inzidenzstruktur. Dann gilt:*
a) *Ist* T *eine linksseitige taktische Konfiguration mit den Parametern* v, r, k_c *mit* $c \in \mathrm{B}$, *so ist* $vr = \sum_{c \in \mathrm{B}} k_c$.
b) *Ist* T *eine rechtsseitige taktische Konfiguration mit den Parametern* b, k, r_p *mit* $P \in \Pi$ *so ist* $bk = \sum_{P \in \Pi} r_P$.
c) *Ist* T *eine taktische Konfiguration mit den Parametern* v, b, r, k, *so ist* $vr = bk$.

Es seien t, v, k und λ natürliche Zahlen. Die Inzidenzstruktur $(\Pi, \mathrm{B}, \mathrm{I})$ heißt t-(v, k, λ)-*Blockplan*, falls gilt:

(1) Es ist $v = |\Pi|$.

(2) Es ist $k_c = k$ für alle $c \in \mathrm{B}$.

(3) Je t verschiedene Punkte aus Π inzidieren mit genau λ Blöcken aus B.

Statt t-(v, k, λ)-Blockplan werden wir häufig nur t-Blockplan sagen und 2-Blockpläne werden wir meist nur Blockpläne nennen.

Die 1-Blockpläne sind genau die taktischen Konfigurationen mit den Parametern v, b, $r = \lambda$ und k. Auf Grund von (2) sind alle t-Blockpläne rechtsseitige taktische Konfigurationen. Wir werden sehen, dass sie stets sogar taktische Konfigurationen sind. Bevor wir dies beweisen, noch eine Definition. Ist $T := (\Pi, \mathrm{B}, \mathrm{I})$ eine Inzidenzstruktur und ist P ein Punkt von T, so definieren wir die *abgeleitete Struktur* T_P wie folgt:

(a) Punkte von T_P sind die von P verschiedenen Punkte von T.

(b) Blöcke von T_P sind die mit P inzidierenden Blöcke von T.

(c) Inzidenz in T_P ist gleichbedeutend mit Inzidenz in T.

Sind $P_1, \ldots, P_n$ verschiedene Punkte von T, so definieren wir $T_{P_1,\ldots,P_n}$ rekursiv vermöge

$$T_{P_1,\ldots,P_n} := (T_{P_1,\ldots,P_{n-1}})_{P_n}.$$

1.3. Satz. *Ist T ein t-(v,k,λ)-Blockplan und ist $1 \leq s \leq t$, so ist T ein s-(v,k,λ_s)-Blockplan, wobei*

$$\lambda_s = \lambda \frac{(v-s)(v-s-1)\cdots(v-t+1)}{(k-s)(k-s-1)\cdots(k-t+1)}$$

ist. Insbesondere ist T auch eine taktische Konfiguration. Ist b die Anzahl der Blöcke von T, so ist

$$b = \lambda \frac{v(v-1)\cdots(v-t+1)}{k(k-1)\cdots(k-t+1)}.$$

Beweis. $P_1, \ldots, P_s$ seien s verschiedene Punkte von T. Wir bezeichnen mit $\lambda(P_1,\ldots,P_s)$ die Anzahl der Blöcke von $T_{P_1,\ldots,P_s}$. Ist $s = t$, so ist $\lambda(P_1,\ldots,P_s) = \lambda$, so dass in diesem Falle $\lambda(P_1,\ldots,P_s)$ von der Auswahl der Punkte $P_1,\ldots,P_s$ unabhängig ist. Es sei $s < t$ und es sei bereits gezeigt, dass es ein λ_{s+1} gibt mit

$$\lambda(X_1,\ldots,X_{s+1}) = \lambda_{s+1}$$

für jede Wahl der $X_1, \ldots, X_{s+1}$. Dann ist $T_{P_1,\ldots,P_s}$ eine taktische Konfiguration mit den Parametern $v_s = v - s$, $b_s = \lambda(P_1,\ldots,P_s)$, $k_s = k - s$ und $r_s = \lambda_{s+1}$. Nach 1.2c) ist $v_s r_s = b_s k_s$. Somit ist

$$\lambda(P_1,\ldots,P_s) = \frac{v-s}{k-s}\lambda_{s+1}.$$

Damit ist gezeigt, dass T auch ein s-(v,k,λ_s)-Blockplan ist. Nun ist $r_P = \lambda_1$ für alle Punkte P von T. Daher ist $v\lambda_1 = bk$ nach 1.2c) und folglich

$$b = \lambda \frac{v(v-1)\cdots(v-t+1)}{k(k-1)\cdots(k-t+1)}.$$

Damit ist alles bewiesen.

Es sei L ein projektiver Verband. Mit $\mathrm{UR}_i(L)$ bezeichnen wir, wie schon zuvor, die Menge der Unterräume des Ranges i von L. Ist L ein endlicher projektiver Verband der Ordnung q und des Ranges n, so bezeichnen wir wieder die Anzahl der Elemente in $\mathrm{UR}_i(L)$ mit $N_i(n,q)$. Für $0 \leq i \leq j \leq n$, setzen wir

$$L_{i,j} := \big(\mathrm{UR}_i(L), \mathrm{UR}_j(L), \leq\big).$$

Es gilt dann:

1.4. Satz. *Es sei L ein endlicher projektiver Verband der Ordnung q und des Ranges n. Ferner seien i und j natürliche Zahlen mit $1 \leq i \leq j \leq n$. Dann gilt:*

a) *$L_{i,j}$ ist eine taktische Konfiguration mit den Parametern $v = N_i(n, q)$, $b = N_j(n, q)$, $k = N_i(j, q)$ und $r = N_{j-i}(n - i, q)$.*

b) *Ist $1 < j$, so ist $L_{1,j}$ ein 2-Blockplan mit $v = N_1(n, q)$, $b = N_j(n, q)$, $k = N_1(j, q)$ und $\lambda = N_{j-2}(n - 2, q)$.*

Beweis. Dass v, b und k die angegebenen Werte haben, folgt aus der Definition der $N_a(b, q)$. Es sei $U \in \mathrm{UR}_i(L)$ und Π sei das größte Element von L. Dann ist die Anzahl der Unterräume vom Range j, die U umfassen, gleich der Anzahl der Unterräume vom Range $j - i$ in dem Quotienten Π/U. Folglich ist diese Anzahl gleich $N_{j-i}(n - i, q)$. Damit ist a) bewiesen.

Dass $N_{j-2}(n-2, q)$ die Anzahl der Unterräume vom Rang j ist, die zwei verschiedene vorgegebene Punkte umfassen, folgt aus a), wenn man nur bemerkt, dass die Summe zweier verschiedener Punkte stets eine Gerade ist. Somit gilt auch b).

1.5. Satz. *Ist L eine projektive Ebene der Ordnung q, so ist $L_{1,2}$ ein 2-$(q^2 + q + 1, q + 1, 1)$-Blockplan. Ist umgekehrt q eine natürliche Zahl mit $q \geq 2$ und ist E ein 2-$(q^2 + q + 1, q + 1, 1)$-Blockplan, so gibt es eine projektive Ebene L, so dass E und $L_{1,2}$ isomorph sind.*

Beweis. Nach I.7.6 ist $N_1(3, q) = q^2+q+1$, $N_1(2, q) = q+1$ und $N_0(1, q) = 1$. Daher ist $L_{1,2}$ auf Grund von 1.4 ein 2-$(q^2 + q + 1, q + 1, 1)$-Blockplan.

Ist umgekehrt E ein 2-$(q^2+q+1, q+1, 1)$-Blockplan mit $q \geq 2$, so trägt jeder Block von E mindestens 3 Punkte und durch zwei verschiedene Punkte geht genau ein Block. Nach 1.3 gehen durch jeden Punkt von E genau $(q^2+q)q^{-1} = q + 1$ Blöcke. Es seien g und h zwei verschiedene Blöcke. Weil zwei Blöcke höchstens einen Punkt gemeinsam haben, gibt es einen Punkt P auf g, der nicht auf h liegt. Auf h liegen $q + 1$ Punkte. Diese sind alle mit P durch genau einen Block verbunden. Diese Blöcke sind allesamt verschieden voneinander, da P nicht auf h liegt. Da P mit genau $q + 1$ Blöcken inzidiert, ist g einer dieser Blöcke. Folglich haben g und h einen Punkt gemeinsam. Da zwei Geraden, wie gerade gesehen, stets einen Punkt gemeinsam haben, gilt auch das Veblen-Young Axiom. Es gibt daher einen projektiven Verband L, so dass E und $L_{1,2}$ isomorph sind. Da zwei verschiedene Geraden von L stets einen Schnittpunkt haben, ist der Rang von L höchstens gleich 3. Weil nicht alle Punkte von L kollinear sind, es ist ja $q^2 + q + 1 > q + 1$, ist der Rang von L aber auch mindestens gleich 3. Somit ist L eine projektive Ebene.

Es sei G eine Gruppe und M sei eine Menge und jedes $g \in G$ wirke als unärer Operator auf M. Wir nennen G *Operatorgruppe* auf M, wenn folgende Bedingungen erfüllt sind.

(j) Es ist $x^{gh} = (x^g)^h$ für alle $x \in M$ und alle $g, h \in G$.

(ij) Es ist $x^1 = x$ für alle $x \in M$.

Ist $x \in M$, so heißt $x^G := \{x^g \mid g \in G\}$ *Bahn* von G. Zwei verschiedene Bahnen haben leeren Durchschnitt. G heißt *transitiv*, falls M eine Bahn ist.

Sind G und M endlich, so gilt, wie auch bei Permutationsgruppen, die Gleichung $|G| = |x^G||G_x|$, wobei $G_x := \{g \mid g \in G,\ x^g = x\}$ ist.

Sind G und M endlich, so bezeichnen wir mit $\chi(g)$ die Anzahl der Fixelemente von $g \in G$. Die Abbildung χ heißt *Permutationscharakter* von G.

1.6. Satz. *Ist G eine endliche Operatorgruppe auf der endlichen Menge M und ist a die Anzahl der Bahnen von G, so ist*

$$a|G| = \sum_{g \in G} \chi(g).$$

Beweis. Wir betrachten die Inzidenzstruktur (M, G, I) mit $x \mathrel{\mathrm{I}} g$ genau dann, wenn $x^g = x$ ist. Dann ist $k_g = \chi(g)$ und $r_x = |G_x|$. Nach 1.1 ist daher $\sum_{g \in G} \chi(g) = \sum_{x \in M} |G_x|$. Es seien $M_1, \ldots, M_a$ die Bahnen von G und x_i sei ein Element aus M_i. Dann ist

$$\sum_{x \in M} |G_x| = \sum_{i:=1}^{a} \sum_{x \in M_i} |G_x| = \sum_{i:=1}^{a} |M_i||G_{x_i}| = \sum_{i:=1}^{a} |G| = a|G|.$$

Damit ist der Satz bewiesen.

1.7. Satz. *Ist G eine endliche Operatorgruppe auf der endlichen Menge M, ist G transitiv auf M und ist b die Anzahl der Bahnen von G_x mit $x \in M$, so ist*

$$b|G| = \sum_{g \in G} \chi(g)^2.$$

Beweis. Weil G transitiv ist, sind die Gruppen G_x für $x \in M$ alle konjugiert. Somit sind G_x und b unabhängig von $x \in M$. Wir betrachten die Inzidenzstruktur $(M \times M, G, \mathrm{I})$, wobei genau dann $(x, y) \mathrel{\mathrm{I}} g$ gilt, wenn $x^g = x$ und $y^g = y$ ist. Es ist dann $k_g = \chi(g)^2$ und $r_{(x,y)} = |G_{x,y}|$. Nach 1.1 ist daher

$$\sum_{g \in G} \chi(g)^2 = \sum_{x \in M} \sum_{y \in M} |G_{x,y}|.$$

Ersetzt man im Beweise von 1.6 die Gruppe G durch die Gruppe G_x, so zeigt die letzte Zeile dieses Beweises, dass $\sum_{y \in M} |G_{x,y}| = b|G_x|$ ist. Also ist

$$\sum_{g \in G} \chi(g)^2 = b \sum_{x \in M} |\ G_x| = b|M||G_x| = b|G|,$$

q. o. o.

2. Inzidenzmatrizen

Es sei T eine endliche Inzidenzstruktur, $P_1, \ldots, P_v$ seien ihre Punkte und $c_1, \ldots, c_b$ ihre Blöcke. Wir definieren die $(v \times b)$-Matrix A durch

$$A_{ij} := \begin{cases} 1, & \text{falls } P_i \mathrel{\mathrm{I}} c_j \\ 0, & \text{falls } P_i \mathrel{\not\mathrm{I}} c_j. \end{cases}$$

Die Matrix A heißt *Inzidenzmatrix* von T. Mit E bezeichnen wir die $(v \times v)$-Einheitsmatrix und mit J die $(v \times v)$-Matrix, deren sämtliche Einträge gleich 1 sind. Schließlich bezeichne A^t die zu A transponierte Matrix.

2.1. Satz. *Ist A Inzidenzmatrix eines 2-(v, k, λ)-Blockplanes T und ist r die Anzahl der Blöcke durch einen Punkt von T, so ist $AA^t = (r - \lambda)E + \lambda J$.*

Beweis. Der Punkt P_i inzidiert mit genau r Blöcken. Daher sind von den Zahlen A_{ij} für $j := 1, \ldots, b$ genau r gleich 1, während alle übrigen Null sind. Daher ist einmal $A_{ij}^2 = A_{ij}$ und weiter

$$r = \sum_{j:=1}^{b} A_{ij} = \sum_{j:=1}^{b} A_{ij}^2.$$

Folglich sind die Diagonalelemente von AA^t alle gleich r. Ist $i \neq j$, so ist genau dann $A_{ik}A_{jk} \neq 0$, wenn $A_{ik} = A_{jk} = 1$ ist, dh., genau dann, wenn P_i, P_j I c_k gilt. Weil zwei verschiedene Punkte mit genau λ Blöcken inzidieren, ist daher

$$\sum_{k:=1}^{b} A_{ik}A_{jk} = \lambda,$$

falls nur $i \neq j$ ist. Damit ist 2.1 bewiesen.

2.2. Satz. *Es seien a und b zwei reelle Zahlen und es sei $B := (a - b)E + bJ$ eine $(v \times v)$-Matrix. Dann gilt:*

a) *Die Eigenwerte von B sind $a + (v - 1)b$ und $a - b$. Die Vielfachheit von $a + b(v - 1)$ ist 1 und die Vielfachheit von $a - b$ ist $v - 1$.*

b) *Es ist* $\det(B) = (a + (v - 1)b)(a - b)^{v-1}$.

Beweis. Es sei E_v das v-Tupel aus lauter Einsen. Ferner sei für $i := 1, \ldots, v - 1$ das v-Tupel E_i erklärt durch

$$E_{ij} := \begin{cases} 1, & \text{falls } j = i \\ -1, & \text{falls } j = i + 1 \\ 0 & \text{sonst.} \end{cases}$$

Dann ist

$$BE_v = (a - b)EE_v + bJE_v = (a - b)E_v + bvE_v = \big(a + (v - 1)b\big)E_v$$

und für $i < v$ ist

$$BE_i = (a - b)EE_i + bJE_i = (a - b)E_i.$$

Weil die Charakteristik von $\mathbf{R}$ Null ist, sind die Vektoren $E_1, \ldots, E_v$ linear unabhängig. Folglich gilt a).

Die Aussage b) ist eine unmittelbare Folgerung aus a).

2.3. Korollar. *Ist A die Inzidenzmatrix eines 2-(v, k, λ)-Blockplanes und ist $k < v$, so ist der Rang von A gleich v.*

Beweis. Ist r die Anzahl der Blöcke durch einen Punkte des fraglichen Blockplanes, so gilt nach 1.3 die Gleichung $r(k-1) = \lambda(v-1)$. Wegen $k < v$ ist daher $\lambda < r$. Aus 2.1 und 2.2 folgt somit

$$\det(AA^t) = \big(r + (v-1)\lambda\big)(r-\lambda)^{v-1} \neq 0.$$

Weil A eine $(v \times b)$- und AA^t eine $(v \times v)$-Matrix ist, ist daher

$$v \geq \mathrm{Rg}(A) \geq \mathrm{Rg}(AA^t) = v,$$

woraus die Behauptung folgt.

Wir ziehen sofort Nutzen aus diesem Korollar.

2.4. Fishersche Ungleichung. *Ist b die Anzahl der Blöcke eines 2-(v,k,λ)-Blockplanes und ist $k < v$, so ist $v \leq b$.*

Beweis. Ist A eine Inzidenzmatrix eines solchen Blockplanes, so ist A eine $(v \times b)$-Matrix. Nach 2.3 ist daher $b \geq \mathrm{Rg}(A) = v$, q. e. d.

2.5. Satz. *Ist T eine Inzidenzstruktur mit den Eigenschaften*
a) *T besitzt genau v Punkte und genau v Blöcke,*
b) *Jeder Block von T inzidiert mit genau k Punkten,*
c) *zwei verschiedene Blöcke haben genau λ Punkte gemeinsam,*
d) *Es ist $\lambda < k$,*
so ist T ein 2-(v,k,λ)-Blockplan.

Beweis. Es sei A eine Inzidenzmatrix von T. Dann folgt mit b) und c), dass

$$A^tA = (k-\lambda)E + \lambda J$$

ist. Nach 2.2 b) ist daher

$$\det(A^tA) = \big(k + (v-1)\lambda\big)(k-\lambda)^{v-1}.$$

Weil $\lambda < k$ ist, ist daher $\det(A^tA) \neq 0$. Also ist auch $\det(A) \neq 0$. Folglich ist A regulär und A^{-1} existiert. Aus b) folgt, dass $JA = kJ$ ist. Somit ist $k^{-1}J = JA^{-1}$. Weiterhin ist

$$JA^tA = (k-\lambda)JE + \lambda J^2 = (k - \lambda + \lambda v)J.$$

Daher ist

$$JA^t = (k-\lambda+\lambda v)JA^{-1} = k^{-1}(k-\lambda+\lambda v)J.$$

Transponieren liefert

$$AJ = k^{-1}(k-\lambda+\lambda v)J$$

ist. Also ist

$$JAJ = k^{-1}v(k-\lambda+\lambda v)J.$$

Andererseits ist

$$JAJ = (JA)J = kJ^2 = kvJ.$$

Folglich ist $k^{-1}v(k-\lambda+\lambda v) = kv$ und daher $k = k^{-1}(k-\lambda+\lambda v)$. Somit ist

$$AJ = k^{-1}(k-\lambda+\lambda v)J = kJ = JA.$$

Hieraus folgt

$$AA^t = A(A^tA)A^{-1} = A((k-\lambda)E+\lambda J)a^{-1} = (k-\lambda)E+\lambda J).$$

Dies besagt schließlich, dass zwei verschiedene Punkte von T mit genau λ Blöcken inzidieren, q. e. d.

Wir nennen einen 2-Blockplan T *projektiv*, falls die Anzahl seiner Blöcke gleich der Anzahl seiner Punkte ist und falls kein Block von T mit allen Punkten von T inzidiert.

2.6. Korollar *Es sei T ein 2-(v,k,λ)-Blockplan mit $k < v$. Genau dann ist T projektiv, wenn T^d ein 2-Blockplan ist. Ist T projektiv, so ist T^d ebenfalls ein 2-(v,k,λ)-Blockplan.*

Beweis. Es sei T ein 2-(v,k,λ) Blockplan. Dann ist $v \leq b$ auf Grund der fisherschen Ungleichung. Ist T^d ein 2-Blockplan, so ist ebenfalls auf Grund dieser Ungleichung $b \leq v$. Also ist $v = b$ und T ist projektiv.

Es sei umgekehrt T projektiv. Aus $v = b$ und $vr = bk$ folgt dann $r = k$. Folglich erfüllt T^d die Voraussetzungen von 2.5. Also ist T^d ein 2-(v,k,λ)-Blockplan. Damit ist alles bewiesen.

Die Inzidenzstrukturen $L_{1,n-1}$, wobei L ein endlicher projektiver Verband des Ranges $n \geq 3$ ist, sind Beispiele für projektive Blockpläne.

Das nächste Korollar folgt unmittelbar aus 2.6 und 2.1.

2.7. Korollar *Jede Inzidenzmatrix A eines projektiven Blockplanes ist normal, dh. es ist $AA^t = A^tA$.*

3. Kollineationen von projektiven Blockplänen

Es sei Q eine $(n \times n)$-Matrix mit $Q_{ij} \in \{0,1\}$. Die Matrix Q heißt *Permutationsmatrix*, falls $QQ^t = E$ ist. Ist Q eine Permutationsmatrix, so ist Q regulär und es gilt $Q^{-1} = Q^t$. Folglich ist auch $Q^tQ = E$. Aus $QQ^t = Q^tQ = E$ folgt, dass in jeder Zeile und in jeder Spalte von Q genau eine 1 steht. Ist Q eine Permutationsmatrix und definieren wir π durch $i^\pi := j$ genau dann, wenn $Q_{ij} = 1$ ist, so ist $\pi \in S_n$, falls S_n wieder die symmetrische Gruppe vom Grade n bezeichnet. Ist umgekehrt $\pi \in S_n$ und definiert man $Q(\pi)$ durch

$$Q(\pi)_{ij} := \begin{cases} 1, & \text{falls } i^\pi = j, \\ 0, & \text{falls } i^\pi \neq j, \end{cases}$$

so ist $Q(\pi)$ eine Permutationsmatrix. Die so definierte Abbildung Q ist, wie man sich leicht überzeugt, ein Monomorphismus von S_n in die Gruppe der regulären $(n \times n)$-Matrizen, so dass also die Permutationsmatrizen bezüglich der Matrizenmultiplikation eine zu S_n isomorphe Gruppe bilden. Hieraus folgt,

dass jede Permutationsmatrix endliche Ordnung hat, so dass die Eigenwerte einer Permutationsmatrix Einheitswurzeln sind.

3.1. Satz. *Es seien T und T' isomorphe Inzidenzstrukturen. $P_1, \ldots, P_v$ seien die Punkte und $c_1, \ldots, c_b$ seien die Blöcke von T und A sei die zu dieser Nummerierung der Punkte und Blöcke gehörende Inzidenzmatrix von T. Ferner seien $P'_1, \ldots, P'_v$ die Punkte und $c'_1, \ldots, c'_b$ seien die Blöcke von T' und A' sei die zugehörige Inzidenzmatrix von T'. Ist σ ein Isomorphismus von T auf T', so definieren wir die $(v \times v)$-Permutationsmatrix $Q(\sigma)$ durch*

$$Q(\sigma)_{ij} := \begin{cases} 1, & \textit{falls } P_i^\sigma = P'_j, \\ 0, & \textit{falls } P_i^\sigma \neq P'_j, \end{cases}$$

und die $(b \times b)$-Permutationsmatrix $R(\sigma)$ durch

$$R(\sigma)_{ij} := \begin{cases} 1, & \textit{falls } c_i^\sigma = c'_j, \\ 0, & \textit{falls } c_i^\sigma \neq c'_j. \end{cases}$$

Es gilt dann:

a) *Die Abbildung $\sigma \to (Q(\sigma), R(\sigma))$ ist eine Bijektion der Menge der Isomorphismen von T auf T' auf die Menge der Paare (Q, R) von $(v \times v)$- bzw. $(b \times b)$-Permutationsmatrizen mit $PA' = AQ$.*

b) *Ist $T = T'$ sowie $P_i = P'_i$ und $c_j = c'_j$ für alle in Frage kommenden i und j und sind σ und τ Automorphismen von T, so ist $Q(\sigma\tau) = Q(\sigma)Q(\tau)$ und $R(\sigma\tau) = R(\sigma)r(\tau)$.*

Beweis. a) Es sei σ ein Isomorphismus von T auf T'. Dann ist

$$\big(Q(\sigma)A'\big)_{ij} = \sum_{k:=1}^{v} Q(\sigma)_{ik} A'_{kj} = A'_{fj},$$

wobei f durch $P_i^\sigma = P'_f$ bestimmt ist. Andererseits ist

$$\big(AR(\sigma)\big)_{ij} = \sum_{k:=1}^{b} A_{ik} R(\sigma)_{kj} = A_{ig},$$

wobei g durch $c_g^\sigma = c'_j$ bestimmt ist. Die Frage ist also, ob $A'_{fj} = A_{ig}$ ist. Nun ist $P_i^\sigma = P'_f$ und $c_g^\sigma = c'_j$. Weil σ ein Isomorphismus ist, gilt daher $P_i \mathrel{\mathrm{I}} c_g$ genau dann, wenn $P_i^\sigma \mathrel{\mathrm{I}} c_g^\sigma$, dh., es ist $A_{ig} = 1$ genau dann, wenn $A'_{fj} = 1$ ist. dies zeigt, dass $Q(\sigma)A' = AR(\sigma)$ ist. Also ist $\sigma \to (Q(\sigma), R(\sigma))$ eine Abbildung in die fragliche Menge, die offensichtlich auch injektiv ist.

Um zu zeigen, dass sie auch surjektiv ist, seien C und D Permutationsmatrizen mit $CA' = AD$. Wir definieren σ durch $P_i^\sigma := P'_j$, falls $C_{ij} = 1$ ist, und entsprechend $c_i^\sigma := c_j$ falls $D_{ij} = 1$ ist. Weil C und D Permutationsmatrizen sind, ist σ eine bijektive Abbildung der Menge der Punkte von T auf die Menge der Punkte von T' und der Menge der Blöcke von T auf die Menge der Blöcke

von T'. Es sei $P_i^\sigma = P'_f$ und $c_g^\sigma = c'_j$. Dann ist

$$A_{ig} = \sum_{k:=1}^{b} A_{ik} D_{kj} = \sum_{k:=1}^{v} C_{ik} A'_{kj} = A'_{fj}.$$

Hieraus folgt, dass σ inzidenztreu ist. Es ist klar, dass dann auch $(Q(\sigma), R(\sigma)) = (C, D)$ gilt, womit die Surjektivität nachgewiesen ist. Damit ist a) bewiesen.

Es seien σ und τ Automorphismen von T. Dann ist

$$\big(Q(\sigma)Q(\tau)\big)_{ij} = \sum_{k:=1}^{v} Q(\sigma)_{ik} Q(\tau)_{kj} = Q(\sigma)_{if} Q(\tau)_{fj} = Q(\tau)_{fj},$$

wobei f durch $P_i^\sigma = P_f$ bestimmt ist. Nun gilt genau dann die Ungleichung $(Q(\sigma)Q(\tau))_{ij} \neq 0$, wenn $P_f^\tau = P_j$, dh. genau dann, wenn $P_i^{\sigma\tau} = P_j$ ist. Also ist $Q(\sigma)Q(\tau)_{ij} = Q(\sigma\tau)_{ij}$. Ebenso beweist man die Multiplikativität von R.

3.2. Satz. *Jeder Automorphismus eines projektiven Blockplanes hat ebenso viele Fixpunkte wie Fixblöcke.*

Beweis. Es sei T ein projektiver Blockplan und A sei eine Inzidenzmatrix von T. Ferner sei σ ein Automorphismus von T. Dann ist $\mathrm{Spur}(Q(\sigma)) = \sum_{i:=1}^{v} Q(\sigma)_{ii}$ die Anzahl der Fixpunkte von σ. Entsprechend ist $\mathrm{Spur}(R(\sigma))$ die Anzahl der Fixblöcke von σ. Nun ist $Q(\sigma)A = AR(\sigma)$ und A ist nach 2.3 regulär. Also ist $Q(\sigma) = AR(\sigma)A^{-1}$ und daher $\mathrm{Spur}(Q(\sigma)) = \mathrm{Spur}(R(\sigma))$.

Ist σ eine Permutation auf der Menge M und τ eine solche auf der Menge N, so heißen σ und τ *ähnlich*, wenn es eine Bijektion β von M auf N gibt mit $\sigma = \beta\tau\beta^{-1}$. Entsprechend wird die Ähnlichkeit von Permutationsgruppen definiert.

3.3. Satz. *Ist Z eine zyklische Gruppe von Automorphismen des projektiven Blockplanes T, so ist die Darstellung von Z als Permutationsgruppe auf der Menge der Punkte von T ähnlich zu der Darstellung von Z auf der Menge der Blöcke.*

Beweis. Es genügt zu zeigen, dass für alle n die Anzahl i_n der Punktbahnen der Länge n gleich der Anzahl i'_n der Blockbahnen der Länge n ist.

Ist $i_n \neq 0$, so gibt es eine Bahn der Länge n. Es folgt, dass n Teiler von $|Z|$ ist. Ist n kein Teiler von $|Z|$, so ist $i_n = 0$ und natürlich auch $i'_n = 0$. In diesem Falle ist also $i_n = i'_n$.

Es sei also n Teiler von $|Z|$. Ferner sei ζ ein erzeugendes Element von Z. Dann ist i_1 die Anzahl der Fixpunkte und i'_1 die Anzahl der Fixblöcke von ζ. Nach 3.2 ist $i_1 = i'_1$. Es sei also $n > 1$ und es gelte, dass $i_x = i'_x$ ist für alle $x < n$. Die Anzahl der Fixpunkte von ζ^n ist

$$\sum_{x \text{ teilt } n} x i_x$$

und die Anzahl der Fixblöcke von ζ^n ist

$$\sum_{x \text{ teilt } n} x i'_x.$$

Nach 3.2 sind diese beiden Zahlen aber gleich. Auf Grund unserer Induktionsannahme folgt daher $ni_n = ni'_n$ und weiter $i_n = i'_n$. Damit ist das Korollar bewiesen.

Dass man in 3.3 auf eine Annahme wie die, dass Z zyklisch ist, nicht verzichten kann, sieht man am Beispiel der Gruppe $\mathrm{E}(H, H)$. Diese hat nur eine Fixhyperebene, nämlich H, lässt jedoch alle Punkte von H fest.

Der nächste Satz, der ebenfalls eine Folgerung aus 3.2 ist, wird häufig Satz von Dembowski–Hughes–Parker genannt. Er wurde jedoch schon 1941 von Richard Brauer bewiesen (Brauer 1941, Lemma 3), also vierzehn Jahre vor den Publikationen von Dembowski, Hughes und Parker. Dieser Satz lässt sich auf beliebige Blockpläne verallgemeinern. Dies wird in Satz 5.5 geschehen.

3.4. Satz. *Ist G eine Gruppe von Automorphismen eines projektiven Blockplanes T, so hat G ebenso viele Punkt- wie Blockbahnen. Insbesondere ist G genau dann punkttransitiv, wenn G blocktransitiv ist.*

Beweis. Es sei a_1 die Anzahl der Punkt- und a_2 die Anzahl der Blockbahnen von G. Ferner sei χ_1 der Permutationscharakter von G aufgefasst als Operatorgruppe auf der Menge der Punkte von T und χ_2 sei der Permutationscharakter von G aufgefasst als Operatorgruppe auf der Menge der Blöcke von T. Nach 3.2 ist dann $\chi_1(g) = \chi_2(g)$ für alle $g \in G$. Nach 1.6 ist daher

$$a_1|G| = \sum_{g \in G} \chi_1(g) = \sum_{g \in G} \chi_2(g) = a_2|G|$$

und somit $a_1 = a_2$.

3.5. Satz. *Es sei G eine punkttransitive oder blocktransitive Automorphismengruppe eines projektiven Blockplanes T. Ist P ein Punkt und c ein Block von T, so hat G_P ebenso viele Punktbahnen wie G_c Blockbahnen. Insbesondere Ist G genau dann zweifach transitiv auf der Menge der Punkte von T, wenn G zweifach transitiv auf der Menge der Blöcke von T ist.*

Beweis. Ist G punkttransitiv, so ist G nach 3.4 auch blocktransitiv und umgekehrt. Ist b_1 die Anzahl der Punktbahnen von G_P und b_2 die Anzahl der Blockbahnen von G_c, so ist nach 1.7 und 3.2 also

$$b_1|G| = \sum_{g \in G} \chi_1(g)^2 = \sum_{g \in G} \chi_2(g)^2 = b_2|G|$$

und daher $b_1 = b_2$, q. o. o.

4. Korrelationen von projektiven Blockplänen

Ist $T := (\Pi, \Lambda, \mathrm{I})$ eine Inzidenzstruktur und ist κ ein Isomorphismus von T auf T^d, so heißt κ *Korrelation* von T. Eine Korrelation κ ist also eine Bijektion von Π auf Λ und von Λ auf Π mit der Eigenschaft, dass genau dann $P \mathrel{\mathrm{I}} c$ gilt, wenn $P^\kappa \mathrel{\mathrm{I}^d} c^\kappa$, dh. genau dann, wenn $c^\kappa \mathrel{\mathrm{I}} P^\kappa$ gilt. Ist κ eine Korrelation, so ist κ^2 ein Automorphismus von T. Ist $\kappa^2 = 1$, so heißt κ *Polarität*.

Ist κ eine Korrelation von T und ist P ein Punkt von T mit $P \mathrel{\mathrm{I}} P^\kappa$, so heißt P *absoluter Punkt* von κ. Entsprechend heißt der Block c *absolut*, wenn $c^\kappa \mathrel{\mathrm{I}} c$ ist.

4.1. Satz. *Ist κ eine Korrelation des projektiven Blockplanes T, so hat κ ebenso viele absolute Punkte wie absolute Blöcke.*

Beweis. Es sei a die Anzahl der absoluten Punkte und A die Anzahl der absoluten Blöcke von κ. Ist $P \mathrel{\mathrm{I}} P^\kappa$, so ist $(P^\kappa)^\kappa \mathrel{\mathrm{I}} P^\kappa$. Folglich ist P^κ ein absoluter Block, woraus folgt, dass $a \leq A$ ist. Ist umgekehrt $c^\kappa \mathrel{\mathrm{I}} c$, so ist $c^\kappa \mathrel{\mathrm{I}} (c^\kappa)^\kappa$, so dass c^κ ein absoluter Punkt ist. Daher ist $A \leq a$. Damit ist alles bewiesen.

Ist A eine Inzidenzmatrix der Inzidenzstruktur T, so ist A^t eine Inzidenzmatrix von T^d. Ist κ eine Korrelation von T, so ist nach 3.1 also $Q(\kappa)A^t = AR(\kappa)$. Nummeriert man die Blöcke von T so, dass $c_i = P_i^\kappa$ ist, so ist $Q(\kappa) = E$ und daher $AR(\kappa) = A^t$. Nun ist genau dann $A_{ii} = 1$, wenn $P_i \mathrel{\mathrm{I}} c_i = P_i^\kappa$ ist. Somit ist $\mathrm{Spur}(A)$ die Anzahl der absoluten Punkte von κ.

4.2. Satz. *Es sei T ein projektiver 2-(v,k,λ)-Blockplan. Ferner sei $k - \lambda = ns^2$ mit quadratfreiem n. Ist dann a die Anzahl der absoluten Punkte einer Korrelation von T, so ist $a \equiv \lambda \bmod ns$.*

Beweis. Wie wir bereits bemerkten, gibt es eine Inzidenzmatrix A von T und eine Permutationsmatrix R mit $a = \mathrm{Spur}(A)$ und $AR = A^t$. Nach 2.7 ist A normal. Es gibt folglich eine unitäre Matrix U mit $A = \bar{U}^t DU$, wobei D die Diagonalmatrix aus den Eigenwerten $\mu_1, \ldots, \mu_v$ von A ist. Wegen

$$A^t = \bar{A}^t = \bar{U}^t \bar{D}^t U = \bar{U}^t \bar{D} U$$

sind $\bar{\mu}_1, \ldots, \bar{\mu}_v$ die Eigenwerte von A^t. Weil U unitär ist, ist $U\bar{U}^t = E$. Weil die Koeffizienten von A reell sind, ist daher

$$AA^t = \bar{U}^t DU\bar{U}^t \bar{D}U = \bar{U}^t D\bar{D}U.$$

Somit sind die $\mu_i\bar{\mu}_i$ die Eigenwerte von AA^t. Die Zeilensummen von A sind alle gleich k, so dass k ein Eigenwert von A ist. Wir dürfen annehmen, dass $\mu_1 = k$ ist. Dann ist $\mu_1\bar{\mu}_1 = k^2 = k + \lambda(v-1)$. Aus 2.2 a) folgt dann, dass $\mu_i\bar{\mu}_i = k - \lambda$ ist für $i := 2, \ldots, v$. Setze $m := k - \lambda$. Dann ist $\mu_i = \epsilon_i\sqrt{m}$ und $\epsilon_i\bar{\epsilon}_i = 1$. Weil A regulär ist, folgt $R = A^{-1}A^t$. Hieraus folgt, dass die $\bar{\mu}_i\mu_i^{-1}$ die Eigenwerte von R sind. Nun ist $\bar{\mu}_1\mu_1^{-1} = 1$ und $\bar{\mu}_i\mu_i^{-1} = \epsilon_i^{-2}$ für $i := 2, \ldots, v$. Weil R eine Permutationsmatrix ist, sind die Eigenwerte von R Einheitswurzeln. Hieraus folgt wiederum, dass die ϵ_i Einheitswurzeln sind. Folglich ist $(\sum_{i:=1}^v \epsilon_i)^2$ eine ganz algebraische Zahl. Nun ist

$$(a-k)^2 = \bigl(\mathrm{Spur}(A) - k\bigr)^2 = \Biggl(\sum_{i:=2}^{v} \mu_i\Biggr)^2 = m\Biggl(\sum_{i:=2}^{v} \epsilon_i\Biggr)^2.$$

Somit ist $(\sum_{i:=2}^v \epsilon_i)^2$ rational und als ganz algebraische Zahl sogar ganz rational. Also ist $(a-k)^2 \equiv 0 \bmod m$ und folglich $a \equiv k \bmod ns$. Wegen $k = m + \lambda$ folgt hieraus $a \equiv \lambda \bmod ns$, q. o. o.

Die Begriffe *absoluter Punkt* und *absolute Hyperebene* einer Korrelation eines projektiven Verbandes wurden in Abschnitt 4 von Kapitel II definiert.

4.3. Korollar *Es sei L ein endlicher projektiver Verband mit $r := \mathrm{Rg}(L) \geq 3$.*
a) *Ist κ eine Korrelation von $L_{1,r-1}$, so hat κ wenigstens einen absoluten Punkt.*
b) *Ist κ eine Korrelation von L, so hat κ wenigstens einen absoluten Punkt.*

Beweis. Da jede Korrelation von L eine Korrelation in $L_{1,r-1}$ induziert, genügt es, a) zu beweisen.

Es sei q die Ordnung von L. Nach 1.4 b) ist dann $k = \sum_{i:=0}^{r-2} q^i$ und $\lambda = \sum_{i:=0}^{r-3} q^i$. Daher ist $m = k - \lambda = q^{r-2}$. Ist $m = ns^2$ mit quadratfreiem n und ist p ein Primteiler von q, so ist p ein Teiler von ns. Ferner ist $\lambda \equiv 1 \bmod p$, so dass nach 4.2 die Kongruenz $a \equiv 1 \bmod p$ gilt. Hieraus folgt $a \geq 1$, q. e. d.

Es sei V ein Vektorraum über dem kommutativen Körper K. Die Abbildung Q von V in K heißt *quadratische Form* auf V, falls gilt:
(1) Es ist $Q(vk) = Q(v)k^2$ für alle $v \in V$ und alle $k \in K$.
(2) Die durch $f(u,v) := Q(u+v) - Q(u) - Q(v)$ definierte Abbildung f von $V \times V$ in K ist bilinear.

Als Anwendung von 4.3 beweisen wir den folgenden, rein algebraischen Satz über quadratische Formen über endlichen Körpern.

4.4. Satz. *Es sei V ein Vektorraum über $\mathrm{GF}(q)$ und Q sei eine quadratische Form auf V. Ist $U \in L(V)$ und ist $3 \leq \mathrm{Rg}_K(U) < \infty$, so gibt es ein $u \in U$ mit $u \neq 0$ und $Q(u) = 0$.*

Beweis. Wir betrachten zunächst den Fall, dass die Charakteristik von $\mathrm{GF}(q)$ gleich 2 ist. Ferner sei $u \in U$ und $Q(u) \neq 0$. Wegen $0 = f(0,0) = Q(0) - 2Q(0) = Q(0)$ ist $u \neq 0$. Definiert man g durch $g(x) := f(u,x)$ für alle $x \in U$, so ist g nach (2) eine lineare Abbildung von U in $\mathrm{GF}(q)$. Nun ist $\mathrm{Rg}(U) \geq 3$ und daher $\mathrm{Rg}(\mathrm{Kern}(g)) \geq 2$. Es gibt folglich ein $x \in U$ mit $x \notin u\mathrm{GF}(q)$ und $g(x) = 0$. Es sei $k \in \mathrm{GF}(q)$. Dann ist

$$0 = g(x)k = f(x,u)k = f(x,uk) = Q(x+uk) - Q(x) - Q(uk)$$

und daher

$$Q(x+uk) = Q(x) + Q(u)k^2.$$

Nun ist $\mathrm{GF}(q) = \mathrm{GF}(q)^2$, da die Charakteristik von $\mathrm{GF}(q)$ ja 2 ist. Weil außerdem $Q(u) \neq 0$ ist, gibt es ein $k \in \mathrm{GF}(q)$ mit $Q(x+uk) = 0$. Wäre $x + uk = 0$, so wäre $x \in u\mathrm{GF}(q)$, was nicht der Fall ist. Damit ist 4.4 für den Fall, dass $\mathrm{GF}(q)$ die Charakteristik 2 hat, bewiesen.

Die Charakteristik von $\mathrm{GF}(q)$ sei nun von 2 verschieden. Wir nehmen an, dass $f(u,u) \neq 0$ sei für alle u mit $0 \neq u \in U$. Die Einschränkung von f auf U ist dann eine nicht ausgeartete Bilinearform auf V und definiert somit nach II.8.4 eine Korrelation κ in $L(U)$. Wegen $\mathrm{Rg}_K(U) \geq 3$ gibt es daher nach 4.3 einen absoluten Punkt wU in $L(U)$. Es folgt $0 \neq w$ und $f(w,w) = 0$. Es gibt also doch ein $u \in U$ mit $u \neq 0$ und $f(u,u) = 0$. Es folgt

$$0 = f(u,u) = Q(u+u) - Q(u) - Q(u) = 4Q(u) - 2Q(u) = 2Q(u)$$

und daher $Q(u) = 0$, da die Charakteristik von $\mathrm{GF}(q)$ ja ungleich 2 ist. Damit ist alles bewiesen.

Im Falle einer Polarität kann man mehr über die Anzahl der absoluten Punkte aussagen. Es gilt nämlich:

4.5. Satz. *Ist T ein projektiver 2-(v,k,λ)-Blockplan und ist π eine Polarität von T, so ist die Anzahl der absoluten Punkte von π gleich $k + s\sqrt{k-\lambda}$, wobei s eine geeignete ganze Zahl ist.*

Beweis. $P_1, \ldots, P_v$ seien die Punkte von T. Die Blöcke von T nummerieren wir so, dass $c_i = P_i^\pi$ ist. Für die zu dieser Nummerierung gehörende Inzidenzmatrix gilt dann wegen $\pi^2 = 1$, dass $A = A^t$ ist. Ferner ist $\mathrm{Spur}(A)$ wieder die Anzahl der absoluten Punkte von π. Wie wir bereits wissen, ist k ein Eigenwert von A und die übrigen Eigenwerte von A sind von der Form $\epsilon_i\sqrt{k-\lambda}$ mit $|\epsilon_i| = 1$. Weil A symmetrisch ist, sind die Eigenwerte von A alle reell. Daher ist $\epsilon_i \in \{1, -1\}$. Hieraus folgt alles weitere, da die Spur von A ja gleich der Summe über die Eigenwerte von A ist.

4.6. Korollar. *Ist T ein projektiver 2-(v,k,λ)-Blockplan, ist $k-\lambda$ kein Quadrat und ist π eine Polarität von T, so ist die Anzahl der absoluten Punkte von π gleich k.*

5. Taktische Zerlegungen

Es sei A eine $(v \times b)$-Matrix mit Koeffizienten in einem kommutativen Körper K. Die Zeilen seien dabei mit den Elementen aus $\{1, \ldots, v\}$ und die Spalten mit den Elementen aus $\{1, \ldots, b\}$ indiziert. A sei also das, was ich anderswo ein rechteckiges Schema nannte. Ferner sei $\{Z_1, \ldots, Z_t\}$ eine Partition von $\{1, \ldots, v\}$ mit nicht leeren Z_i und $\{S_1, \ldots, S_{t'}\}$ seien eine Partition von $\{1, \ldots, b\}$ mit nicht leeren S_i. Mit A^{ij} bezeichnen wir die Einschränkung der Abbildung A auf $Z_i \times S_j$. Wir nennen $(Z_1, \ldots, Z_t; S_1, \ldots, S_{t'})$ *linksseitige taktische Zerlegung* von A, falls alle Matrizen A^{ij} konstante Zeilensummen C_{ij} haben. Die Matrix C heißt *assoziierte Zeilensummenmatrix* der linksseitigen taktischen Zerlegung $(Z_1, \ldots, Z_t; S_1, \ldots, S_{t'})$.

Wir nennen $(Z_1, \ldots, Z_t; S_1, \ldots, S_{t'})$ *rechtsseitige taktische Zerlegung* von A, falls die Matrizen A^{ij} konstante Spaltensummen D_{ij} haben. D heißt dann sinngemäß *assoziierte Spaltensummenmatrix* der rechtsseitigen taktischen Zerlegung $(Z_1, \ldots, Z_t;\ S_1, \ldots, S_{t'})$.

Schließlich heißt $(Z_1, \ldots, Z_t; S_1, \ldots, S_t')$ *taktische Zerlegung* der Matrix A, falls $(Z_1, \ldots, Z_t; S_1, \ldots, S_{t'})$ sowohl rechtsseitige als auch linksseitige taktische Zerlegung der Matrix A ist.

Der Leser fragt sich vielleicht, wie man auf solch eine Definition kommt. Das ist hier ausnahmsweise einmal zu beantworten. Nichts ist natürlicher, als die Struktur der Punkt- und Blockbahnen von Kollineationsgruppen von Inzidenzstrukturen zu untersuchen. Nimmt man die Inzidenzstruktur aus einer Punkt- und einer Blockbahn, so sieht man unmittelbar, dass sie eine taktische Konfiguration ist. Verfolgt man nun dies für alle möglichen Paarungen in einer Inzidenzmatrix der fraglichen Inzidenzstruktur, so erhält man eine

taktische Zerlegung der Inzidenzmatrix. Von da ist es dann klar, dass man die Eigenschaften „konstante Zeilensummen“ und „konstante Spaltensummen“ noch separiert. Dies ist in ganz groben Zügen auch die historische Entwicklung, wie sie sich in den Publikationen widerspiegelt.

5.1. Satz. *Es sei A eine $(v \times b)$-Matrix mit Koeffizienten in einem kommutativen Körper. Ferner sei $\{Z_1, \ldots, Z_t\}$ eine Partition von $\{1, \ldots, v\}$ und $\{S_1, \ldots, S_{t'}\}$ eine Partition von $\{1, \ldots, b\}$. Dann gilt:*

a) *Ist $(Z_1, \ldots, Z_t; S_1, \ldots, S'_t)$ eine rechtsseitige taktische Zerlegung von A, ist ρ der Rang von A und ρ_D der Rang der assoziierten Spaltensummenmatrix, so ist*
$$t \leq \rho_D + v - \rho.$$
Insbesondere gilt
$$t \leq t' + v - \rho.$$

b) *Ist $(Z_1, \ldots, Z_t; S_1, \ldots, S_{t'})$ eine linksseitige taktische Zerlegung von A, ist ρ der Rang von A und ρ_C der Rang der assoziierten Zeilensummenmatrix, so ist*
$$t' \leq \rho_C + b - \rho.$$
Insbesondere gilt
$$t' \leq t + b - \rho.$$

Beweis. Ist $(Z_1, \ldots, Z_t; S_1, \ldots, S_{t'})$ eine linksseitige taktische Zerlegung von A und ist C die assoziierte Zeilensummentmatrix, so ist $(S_1, \ldots, S_{t'}; Z_1, \ldots, Z_t)$ eine rechtsseitige taktische Zerlegung von A^t und C^t ist die assoziierte Spaltensummenmatrix dieser Zerlegung. Weil sich die Ränge beim Transponieren nicht ändern, genügt es daher, 5.1a) zu beweisen.

Da ρ der Rang von A ist, gibt es ρ linear unabhängige Zeilenvektoren von A. Die Indizes der übrigen $v-\rho$ Zeilenvektoren liegen in höchstens $v-\rho$ Klassen Z_1, $\ldots$, Z_t. Es gibt also $t-v+\rho$ Klassen in $\{Z_1, \ldots, Z_t\}$, so dass die Zeilenvektoren mit Indizes in der Vereinigung dieser $v-t+\rho$ Klassen linear unabhängig sind. Wir dürfen annehmen, dass dies die Klassen Z_1, $\ldots$, $Z_{v-t+\rho}$ sind. Es seien z_1, $\ldots$, $z_{v-t+\rho}$ die ersten $t-v+\rho$ Zeilenvektoren der assoziierten Spaltensummenmatrix. Ferner sei $\sum_{i:=1}^{t-v+\rho} z_i\lambda_i = 0$ und es sei a_l der l-te Zeilenvektor von A. Dann folgt aus der Definition der rechtsseitigen taktischen Zerlegung, dass
$$\sum_{i:=1}^{t-v+\rho} \sum_{l \in Z_i} a_l \lambda_i = 0$$
ist. Weil die Zeilenvektoren a_l mit $l \in \bigcup_{i:=1}^{t-v+\rho} Z_i$ linear unabhängig sind, ist daher $\lambda_1 = \ldots = \lambda_{t-v+\rho} = 0$. Also ist $t-v+\rho \leq \rho_D$ und folglich $t \leq \rho_D + v - \rho$. Schließlich ist $\rho_D \leq t'$, da ja D eine $(t \times t')$-Matrix ist. Damit ist 5.1 bewiesen.

Und nun zur Anwendung dieses Satzes auf endliche Inzidenzstrukturen. Es sei $T := (\Pi, \Lambda, \mathrm{I})$ eine endliche Inzidenzstruktur. Ferner sei $\{\Pi_1, \ldots, \Pi_t\}$ eine Partition von Π und $\{\Lambda_1, \ldots, \Lambda_{t'}\}$ eine solche von Λ. Wir nennen dann

$(\Pi_1, \dots, \Pi_t; \Lambda_1, \dots, \Lambda_{t'})$ *linksseitige taktische Zerlegung* von T, falls die Inzidenzstrukturen $T^{ij} := (\Pi_i, \Lambda_j, \mathrm{I}_{ij})$ mit

$$\mathrm{I}_{ij} := \mathrm{I} \cap (\Pi_i \times \Lambda_j)$$

für alle i und j linksseitige taktische Konfigurationen sind. Sind die T^{ij} allesamt rechtsseitige taktische Konfigurationen, so heißt die Zerlegung $(\Pi_1, \dots, \Lambda_{t'})$ *rechtsseitige taktische Zerlegung*. Eine Zerlegung, die sowohl rechtsseitig als auch linksseitig ist, heißt *taktische Zerlegung* schlechthin.

5.2. Satz. *Es sei $T := (\Pi, \Lambda, \mathrm{I})$ eine endliche Inzidenzstruktur. $P_1, \dots, P_v$ seien ihre Punkte und $c_1, \dots, c_b$ ihre Blöcke und A sei die zu dieser Nummerierung der Punkte und Blöcke gehörende Inzidenzmatrix. Schließlich sei $\{\Pi_1, \dots, \Pi_t\}$ eine Partition von Π und $\{\Lambda_1, \dots, \Lambda_{t'}\}$ eine Partition von Λ. Wir definieren eine Partition $\{Z_1, \dots, Z_t\}$ von $\{1, \dots, v\}$ sowie eine Partition $\{S_1, \dots, S_{t'}\}$ von $\{1, \dots, b\}$ durch*

$$Z_i := \big\{ i \mid i \in \{1, \dots, v\},\ P_i \in \Pi_i \big\}$$

bzw.

$$S_i := \big\{ i \mid i \in \{1, \dots, b\},\ c_i \in \Lambda_i \big\}.$$

Es gilt dann:

a) *Genau dann ist $(\Pi_1, \dots, \Pi_t; \Lambda_1, \dots, \Lambda_{t'})$ eine linksseitige taktische Zerlegung von T, wenn $(Z_1, \dots, Z_t; S_1, \dots, S_{t'})$ eine linksseitige taktische Zerlegung von A ist.*
b) *Genau dann ist $(\Pi_1, \dots, \Pi_t; \Lambda_1, \dots, \Lambda_{t'})$ eine rechtsseitige taktische Zerlegung von T, wenn $(Z_1, \dots, Z_t; S_1, \dots, S_{t'})$ eine rechtsseitige taktische Zerlegung von A ist.*
c) *Genau dann ist $(\Pi_1, \dots, \Pi_t; \Lambda_1, \dots, \Lambda_{t'})$ eine taktische Zerlegung von T, wenn $(Z_1, \dots, Z_t; S_1, \dots, S_{t'})$ eine taktische Zerlegung von A ist.*

Zum Beweise von 5.2 hat man nur zu bemerken, dass die A^{ij} Inzidenzmatrizen von T^{ij} sind.

Aus 5.1 a), 5.2 und 2.3 folgt unmittelbar

5.3. Korollar. *Ist T ein 2-(v, k, λ)-Blockplan mit $k < v$ und besitzt T eine taktische Zerlegung mit t Punkt- und t' Blockklassen und ist b die Anzahl der Blöcke von T, so ist*

$$t \leq t' \leq t + b - v.$$

Ist T projektiv, so ist $t = t'$.

Dass taktische Zerlegungen projektiver Blockpläne stets ebenso viele Punkt- wie Blockklassen haben, wurde zuerst von P. Dembowski bewiesen. Es ist eines der ersten Resultate über taktische Zerlegungen überhaupt. Die fishersche Ungleichung ist ein Spezialfall von 5.3, da die Zerlegung der Punkt- bzw. Blockmenge von T in einelementige Teilmengen eine taktische Zerlegung von T ist.

Wie oben schon gesagt, war die im folgenden Satz ausgesprochene Bemerkung Ausgangspunkt für alle Untersuchungen über taktische Zerlegungen.

5.4. Satz. *Ist G eine Gruppe von Automorphismen einer endlichen Inzidenzstruktur $T := (\Pi, \Lambda, \mathrm{I})$, sind $\Pi_1, \ldots, \Pi_t$ die Punktbahnen und $\Lambda_1, \ldots, \Lambda_{t'}$ die Blockbahnen von G, so ist*

$$(\Pi_1, \ldots, \Pi_t; \Lambda_1, \ldots, \Lambda_{t'})$$

eine taktische Zerlegung von T.

Beweis. Es ist zu zeigen, dass $T^{ij} := (\Pi_i, \Lambda_j, \mathrm{I}_{ij})$ eine taktische Konfiguration ist. Dies ist aber trivial, da G in T^{ij} eine Gruppe von Automorphismen induziert, die sowohl auf Π_i als auch auf Λ_j transitiv operiert.

Mit 5.4 und 5.3 folgt schließlich die schon angekündigte Verallgemeinerung von 3.4.

5.5. Korollar. *Ist G eine Gruppe von Automorphismen eines endlichen Blockplanes T und ist die Anzahl der Punktbahnen von G gleich t und die Anzahl der Blockbahnen gleich t', so ist*

$$t \leq t' \leq t + b - v.$$

Dabei ist v die Anzahl der Punkte und b die Anzahl der Blöcke von T.

Das Korollar 3.4 folgt auch aus 5.5, da bei projektiven Blockplänen ja $v = b$ und demzufolge $t = t'$ ist.

6. Endliche desarguessche projektive Ebenen

Ist E eine projektive Ebene, so heißt E *Moufangebene*, falls E bezüglich jeder ihrer Geraden Translationsebene ist (siehe Kapitel II, Ende von Abschnitt 1). Alle desarguesschen Ebenen sind somit auch Moufangebenen, aber nicht alle Moufangebenen sind desarguessch (siehe etwa Pickert 1955, S. 176–178). Für endliche projektive Ebenen gilt jedoch

6.1. Satz. *Alle endlichen Moufangebenen sind desarguessch.*

Dieser Satz ist die Grundlage für viele Charakterisierungen der endlichen desarguesschen projektiven Ebenen. Sein Beweis bedarf einiger Vorbereitung. Der Leser beachte, dass bei den Sätzen 6.2 bis 6.14 nicht die Endlichkeit der betrachteten Moufangebenen und Alternativkörper vorausgesetzt wird.

6.2. Satz. *Ist M eine Moufangebene, so ist die von allen Elationen erzeugte Kollineationsgruppe von M auf der Menge der Tripel (P, Q, G), wobei P und Q zwei verschiedene Punkte und G eine Gerade von M ist, die weder P noch Q enthält, transitiv.*

Beweis. Es seien G und G' Geraden von M und P, Q seien zwei verschiedene Punkte von M_G und P', Q' seien zwei verschiedene Punkte von $M_{G'}$. Weil $\mathrm{Rg}(M) = 3$ ist, gibt es einen Punkt $R \leq G \cap G'$. Ferner gibt es eine von G und

G' verschiedene Gerade H durch R. Es sei C ein von R verschiedener Punkt auf H und I eine von H verschiedene Gerade durch C. Definiere X und Y durch $X := G \cap I$ und $Y := G' \cap I$. Dann sind X und Y von C verschiedene Punkte. Weil M eine Moufangebene ist, gibt es ein $\tau \in \mathrm{E}(R,H)$ mit $X^\tau = Y$. Es folgt

$$G^\tau = (X+R)^\tau = Y + R = G'.$$

Wir dürfen daher annehmen, dass $G = G'$ ist. Weil $\mathrm{E}(G)$ auf der Menge der Punkte von E_G transitiv operiert, dürfen wir weiterhin annehmen, dass auch $P = P'$ ist. Wir haben nun zwei Fälle zu unterscheiden.

1. Fall: P, Q und Q' sind nicht kollinear. Dann ist insbesondere $Q \neq Q'$. Daher ist $Q+Q'$ eine Gerade, die wegen $Q \not\leq G$ von G verschieden ist. Somit ist $C := (Q+Q') \cap G$ ein Punkt. Weil $P \not\leq G$ ist, ist auch $P+C$ eine Gerade, die von G verschieden ist. Sie ist aber auch von $Q+Q'$ verschieden, da P, Q, Q' ja nicht kollinear sind. Es gibt folglich ein $\tau \in \mathrm{E}(C, P+C)$ mit $Q^\tau = Q'$. Weil $P^\tau = P$ und wegen $C \leq G$ auch $G^\tau = G$ ist, ist $(P^\tau, Q^\tau, G^\tau) = (P, Q', G) = (P', Q', G')$.

2. Fall: P, Q und Q' sind kollinear. In diesem Fall wählen wir einen Punkt R mit $R \not\leq P+Q$. Dann sind weder P, Q, R noch P, Q', R kollinear. Wie wir im Falle 1 gesehen haben, gibt es dann Elationen σ und τ mit $P^\sigma = P$, $Q^\sigma = R$, $G^\sigma = G$ und $P^\tau = P$, $R^\tau = Q'$, $G^\tau = G$. Dann ist $\sigma\tau$ eine Kollineation aus der von allen Elationen erzeugten Gruppe, die (P,Q,G) auf (P',Q',G') abbildet. Damit ist 6.2 bewiesen.

6.3. Satz. *Ist M eine Moufangebene, ist G eine Gerade von M und sind P und Q zwei verschiedene Punkte von M_G, so gibt es eine involutorische Perspektivität mit der Achse G, die P und Q vertauscht.*

Beweis. Wir zeigen zunächst, dass M eine involutorische Perspektivität mit der Achse G besitzt. Dazu dürfen wir annehmen, dass alle Elationen mit der Achse G eine von 2 verschiedene Ordnung haben. Der Kern $K(G)$ von $\mathrm{E}(G)$, der nach II.2.1 ein Körper ist, hat dann von 2 verschiedene Charakteristik. Hieraus folgt, dass die multiplikative Gruppe von K ein Element der Ordnung 2 enthält, nämlich -1. Nach II.2.1 gibt es folglich eine involutorische Streckung mit der Achse G.

Es sei nun ρ eine involutorische Perspektivität mit der Achse G. Es gibt dann zwei verschiedene Punkte X und Y von M_G mit $X^\rho = Y$ und $Y^\rho = X$. Nach 6.2 gibt es eine Kollineation γ mit $X^\gamma = P, Y^\gamma = Q$ und $G^\gamma = G$. Die Kollineation $\gamma^{-1}\rho\gamma$ ist dann eine involutorische Perspektivität mit der Achse G, die P mit Q vertauscht.

M sei wieder eine Moufangebene. Ferner sei (U,V,O,E) ein Rahmen von M. Die Menge der Punkte auf $O+V$, die von V verschieden sind, bezeichnen wir mit K. Außerdem bezeichnen wir die Elemente von K mit kleinen lateinischen Buchstaben. Schließlich schreiben wir PQ für die Verbindungsgerade $P+Q$ zweier verschiedener Punkte P und Q, da wir dem Pluszeichen in diesem Abschnitt eine andere Bedeutung unterlegen werden, wie gleich erläutert wird. Ist P ein Punkt von M_{UV}, so setzen wir

$$x_P := (PV \cap OE)U \cap OV$$

und

$$y_P := PU \cap OV.$$

Ist umgekehrt $(x, y) \in K \times K$, so definieren wir $\tau(x, y)$ durch

$$\tau(x, y) := (xU \cap OE)V \cap yU.$$

Offensichtlich gilt $\tau(x_P, y_P) = P$ und $x_{\tau(x,y)} = x$ sowie $y_\tau(x, y) = y$. Folglich ist τ eine Bijektion von $K \times K$ auf die Menge der Punkte von M_{UV}. Ferner gilt $\tau^{-1}(P) = (x_P, y_P)$.

Ist G eine Gerade von M_{UV}, die nicht durch V geht, so setzen wir

$$m_G := \big((G \cap UV)O \cap VE\big)U \cap OV$$

und

$$b_G := G \cap OV.$$

Ist umgekehrt $[m, b] \in K \times K$, so setzen wir

$$\gamma[m, b] := \big((mU \cap EV)O \cap UV\big)b.$$

Man sieht wiederum ohne Mühe, dass die Abbildung γ eine Bijektion von $K \times K$ auf die Menge der nicht durch V gehenden Geraden von M ist und dass $\gamma^{-1}(G) = [m_G, b_G]$ ist.

Schließlich definieren wir auf K eine Addition durch

$$x + y := \big((xU \cap OE)V \cap (EO \cap UV)y\big)U \cap OV$$

und eine Multiplikation durch

$$xy := \big((xU \cap EV)O \cap (yU \cap OE)V\big)U \cap OV.$$

6.4. Satz. *Ist $\tau \in \mathrm{E}(UV)$ und ist $O^\tau = \pi(a, b)$, so ist*

$$\tau(x, y)^\tau = \tau(x + a, y + b)$$

für alle $x, y \in K$. Insbesondere ist K bez. der Addition eine zu $\mathrm{E}(V, UV)$ isomorphe Gruppe und O ist das bez. der Addition neutrale Element von K. Wir setzen daher im Folgenden $0 := O$.

Beweis. Es sei zunächst $a = 0$. Dann ist $\tau(a, b) = \tau(0, b) = b$. Ferner ist $y = (yU \cap OE)U \cap OV$ und daher

$$y^\tau = (yU \cap OE)^\tau U \cap OV,$$

da ja $\tau \in \mathrm{E}(V, UV)$ ist. Nun ist

$$(yU \cap OE)^\tau \leq (yU \cap OE)V.$$

Ferner ist

$$yU \cap OE \leq OE = O(OE \cap UV)$$

und somit

$$(yU \cap OE)^\tau \leq O^\tau(OE \cap UV) = b(OE \cap UV).$$

Insgesamt erhalten wir

$$y^\tau = \big((yU \cap OE)V \cap b(OE \cap UV)\big)U \cap OV = y + b.$$

Nun ist $\pi(x,y) = (xU \cap OE)V \cap yU$ und daher

$$\begin{aligned}\pi(x,y)^\tau &= \big((xU \cap OE)V\big)^\tau \cap y^\tau U^\tau \\ &= (xU \cap OE)V \cap (y+b)U \\ &= \pi(x, y+b).\end{aligned}$$

Es sei ρ die nach 6.3 vorhandene involutorische Perspektivität mit der Achse OE, die U mit V vertauscht. Dann ist

$$\begin{aligned}\pi(x,y)^\rho &= \big((xU \cap OE)V \cap yU\big)^\rho \\ &= \big((xU \cap OE)V \cap (yU \cap OE)U\big)^\rho \\ &= (xU \cap OE)U \cap (yU \cap OE)V \\ &= (yU \cap OE)V \cap xU \\ &= \pi(y,x).\end{aligned}$$

Es sei nun $b = 0$. Dann ist $\tau \in \mathrm{E}(U, UV)$ und daher $\rho^{-1}\tau\rho \in \mathrm{E}(V, UV)$. Ferner ist

$$O^{\rho^{-1}} = O^{\tau\rho} = \pi(a,0)^\rho = \pi(0,a).$$

Nach dem bereits erledigten Fall ist also

$$\pi(x,y)^{\tau\rho} = \pi(y,x)^{\rho^{-1}\tau\rho} = \pi(y, x+a) = \pi(x+a, y)^\rho.$$

Also ist $\pi(x,y)^\tau = \pi(x+a, y)$.

Bezeichnet man die Elation aus $\mathrm{E}(U,V)$, die O auf $\pi(a,b)$ abbildet, mit $\tau(a,b)$, so folgt mit dem bereits Bewiesenem

$$O^{\tau(a,0)\tau(0,b)} = \pi(a,0)^{\tau(0,b)} = \pi(a, 0+b) = \pi(a,b) = O^{\tau(a,b)},$$

so dass $\tau(a,b) = \tau(a,0)\tau(0,b)$ ist. Hieraus folgt schließlich

$$\begin{aligned}\pi(x,y)^{\tau(a,b)} &= \pi(x,y)^{\tau(a,0)\tau(0,b)} \\ &= \pi(x+a, y)^{\tau(0,b)} \\ &= \pi(x+a, y+b).\end{aligned}$$

Schließlich ist

$$O^{\tau(0,a)\tau(0,b)} = \pi(0, a+b) = O^{\tau(0,a+b)}.$$

Daher ist $\tau(0,a)\tau(0,b) = \tau(0,a+b)$. Weil die Abbildung $a \to \tau(0,a)$ offensichtlich eine Bijektion von K auf $\mathrm{E}(V,UV)$ ist, folgt somit, dass $(K,+)$ eine zu $\mathrm{E}(V,UV)$ isomorphe Gruppe ist.

6.5. Satz. *Genau dann ist $\pi(x,y) \le \gamma[m,b]$, wenn $y = mx + b$ ist. Ist G eine von UV verschiedene Gerade durch V, so ist genau dann $\pi(x,y) \le G$, wenn $x = (G \cap OE)U \cap OV$ ist.*

Beweis. $\gamma[m,0]$ ist eine Gerade durch O und aus der Definition der Multiplikation in K folgt unmittelbar, dass genau dann $\pi(x,y) \le \gamma[m,0]$ ist, wenn $y = mx$ ist. Es ist $\gamma[m,b]^{\tau(0,-b)} = \gamma[m,0]$. Daher ist wegen 6.4 genau dann $\pi(x,y) \le \gamma[m,b]$, wenn $\pi(x, y-b) \le \gamma[m,0]$ ist. Hieraus folgt, dass $\pi(x,z)$ genau dann auf $\gamma[m,b]$ liegt, wenn $y - b = mx$ ist. Weil K bezüglich der Addition eine Gruppe ist, folgt somit, dass $y = mx + b$ mit $P(x,y) \le \gamma[m,b]$ gleichbedeutend ist.

Die zweite Behauptung des Satzes ist trivial.

Wir setzen im Folgenden $1 := UE \cap OV$.

6.6. Satz. *Es ist $0x = 0 = 0x$ und $1x = x = x1$ für alle $x \in K$.*

Beweis. Es ist

$$0x = \big(OU \cap (xU \cap OE)V\big)U \cap OV = OU \cap OV = 0$$

und

$$x0 = \big((xU \cap EV)O \cap OV\big)U \cap OV = 0.$$

Also gilt $0x = x0 = 0$ für alle $x \in K$.

Es ist

$$\begin{aligned} 1x &= \big(EO \cap (xU \cap OE)V\big)U \cap OV \\ &= (xU \cap OE)U \cap OV = xU \cap OV = x \end{aligned}$$

und

$$\begin{aligned} x1 &= \big((xU \cap EV)O \cap EV\big)U \cap OV \\ &= (xU \cap EV)U \cap OV = xU \cap OV = x. \end{aligned}$$

Damit ist alles bewiesen.

6.7. Satz. *Sind $a, b \in K$ und ist $a \ne 0$, so gibt es eindeutig bestimmte Elemente $x, y \in K$ mit $ax = b$ und $ya = b$.*

Beweis. Wir betrachten die Geraden $\gamma[a,0]$ und $\gamma[0,b]$. Weil $a \ne 0$ ist, sind diese beiden Geraden nicht parallel. Es gibt also einen Punkt $\pi(x,z)$, der sowohl auf $\gamma[a,0]$ als auch auf $\gamma[0,b]$ liegt. Nach 6.6 und 6.5 sowie 6.4 ist daher $z = 0x + b = b$ und $z = ax + 0 = ax$. Also ist $ax = b$. Ist $ax' = b$, so liegt wegen $b = 0x' + b$ der Punkt $\pi(x',b)$ ebenfalls auf den beiden Geraden $\gamma[a,0]$ und $\gamma[0,b]$. Daher ist $\pi(x,b) = \pi(x',b)$ und weiter $x = x'$. Dies zeigt, dass es im Falle $a \ne 0$ genau ein x gibt mit $ax = b$.

Da $a \ne 0$ ist, ist $\pi(a,b) \ne \pi(0,0)$. Es gibt folglich genau eine Gerade G, die $\pi(0,0)$ mit $\pi(a,b)$ verbindet. Aus 6.5 und $a \ne 0$ folgt, dass G nicht durch V geht. Also ist $G = \gamma[y,z]$. Weil O auf G liegt, ist $z = 0$. Daher ist $b = ya$. Somit existiert also ein y mit $b = ya$. Die Einzigkeit der Lösung y folgt aus der Eindeutigkeit der Verbindungsgeraden von O mit $\pi(a,b)$.

6.8. Satz. *Es ist $a(b+c) = ab + ac$ und $(a+b)c = ac + bc$ für alle a, b, $c \in K$.*

Beweis. Wir betrachten die durch $\pi(x,y)^\tau := \pi(x+c,y)$ definierte Abbildung τ. Nach 6.4 ist $\tau \in \mathrm{E}(U,UV)$. Da τ jede Gerade auf eine zu ihr parallele abbildet, ist $\gamma[a,0]^\tau = \gamma[a,d]$. Nun ist $\pi(x,ax) \le \gamma[a,0]$. Daher ist $\pi(x+c,ax] \le \gamma[a,d]$. Folglich ist $ax = a(x+c)+d$ für alle $x \in K$. Mit $x := 0$ folgt, dass $ac+d = 0$ ist. Folglich ist auch $d+ac = 0$ und weiter

$$ax + ac = a(x+c) + d + ac = a(x+c).$$

Mit $x := b$ erhält man hieraus die Gültigkeit der ersten Behauptung des Satzes.

Es sei $a \in K$. Weil $\mathrm{E}(V,OV)$ die von V verschiedenen Punkte von UV transitiv permutiert, gibt es ein $\tau \in \mathrm{E}(V,OV)$ mit $\gamma[0,0]^\tau = \gamma[\alpha,r]$ mit einem geeigneten $r \in K$. Nun ist $O \le \gamma[0,0]$ und $O^\tau = O$. Daher ist $r = 0$, dh., es ist $\gamma[0,0]^\tau = \gamma[a,0]$.

Die Geraden $\gamma[0,0]$ und $\gamma[0,y]$ sind parallel. Daher sind auch die Geraden $\gamma[0,0]^\tau$ und $\gamma[0,y]^\tau$ parallel. Hieraus folgt, dass $\gamma[0,y]^\tau = \gamma[a,y']$ ist. Nun ist $\pi(0,y) \le \gamma[0,y]$ und $\pi(0,y)^\tau = \pi(0,y)$. Folglich ist $y = a0 + y'$ und somit $y = y'$. Es ist also $\gamma[0,y]^\tau = \gamma[a,y]$.

Ist $\pi(x,y)^\tau = \pi(x',y')$, so ist $x = x'$, da τ die Geraden durch V einzeln festlässt. Nun ist $\pi(x,y) \le \gamma[0,y]$ und daher $\pi(x,y') \le \gamma[a,y]$. Es ist also $\gamma' = ax + y$, dh., es ist $\pi(x,y)^\tau = \pi(x,ax+y)$.

Es sei $\gamma[b,0]^\tau = \gamma[b',t]$. Wegen $O^\tau = O \le \gamma[b,0]$ ist $t = 0$. Nun ist $\pi(x,bx) \le \gamma[b,0]$. Hieraus folgt, dass $\pi(x,ax+bx) \le \gamma[b',0]$ ist, so dass für alle $x \in K$ die Gleichung $ax + bx = b'x$ gilt. Mit $x = 1$ erhält man $a + b = b'$ und mit $x = c$ schließlich $ac + bc = (a+b)c$. Damit ist alles bewiesen.

6.9. Satz. *Ist $a'a = 1$, so ist $a'(ab) = b$ für alle $b \in K$.*

Beweis. $\gamma[a,0]$ ist die Verbindungsgerade von O und $\pi(1,a)$ und $\gamma[a',0]$ ist die Verbindungsgerade von O und $\pi(a,1)$. Ist ρ die nach 6.3 existierende Perspektivität mit der Achse OE, die U mit V vertauscht, so ist, wie wir beim Beweise von 6.4 gesehen haben, $\pi(x,y)^\rho = \pi(y,x)$. Wegen $O^\rho = O$ und $\pi(1,a)^\rho = \pi(a,1)$ ist folglich $\gamma[a,0]^\rho = \gamma[a',0]$. Nun ist $\pi(b,ab) \le \gamma[a,0]$ und daher $\pi(ab,b) \le \gamma[a',0]$, so dass also $b = a'(ab)$ gilt, q. e. d.

6.10. Satz. *Ist $a'a = 1$, so ist auch $aa' = 1$. Ist ferner $aa'' = 1$, so ist $a' = a''$. Jedes von Null verschiedene Element von K hat also genau ein Inverses.*

Beweis. Nach 6.9 ist $a'1 = a' = a'(aa')$. Wegen $a' \ne 0$ ist daher $aa' = 1$ Also ist $aa' = aa''$. Weil $a \ne 0$ ist, ist somit $a' = a''$.

Die Existenzaussage des Satzes folgt mit 6.7.

6.11. Satz. *Ist $a \ne 0$, so ist $(ba)a^{-1} = b$ für alle $b \in K$.*

Beweis. Es sei ρ die involutorische Perspektivität mit der Achse EV, die O mit U vertauscht. Da V ein Fixpunkt von ρ ist, permutiert ρ die Geraden durch V unter sich. Ist $\pi(x,y)$ ein Punkt von M_{UV} mit $x \ne 0$, so ist daher $\pi(x,y)^\rho = \pi(\varphi(x),\psi(x,y))$ mit $\varphi(x)$, $\psi(x,y) \in K$. Nun ist $\gamma[0,y] = U\pi(1,y)$. Daher ist, da ja $\pi(1,y) \le EV$ ist, $\gamma[0,y]^\rho = O\pi(1,y)$. Somit ist $\gamma[0,y]^\rho = \gamma[y,0]$. Ferner ist $\pi(x,y) \le \gamma[0,y]$ und folglich $\pi(\varphi(x),\psi(x,y)) \le \gamma[y,0]$. Hieraus folgt, dass $\psi(x,y) = y\varphi(x)$ ist, falls nur $x \ne 0$ ist. Es ist $\gamma[0,1]^\rho = \gamma[1,0]$ und

daher, da ρ involutorisch ist, $\gamma[1,0]^\rho = \gamma[0,1]$. Wegen $\pi(x,x) \in \gamma[1,0]$ ist $\pi(\varphi(x), \psi(x,x)) \leq \gamma[0,1]$, so dass $\psi(x,x) = 1$ ist für alle $x \in K$. Ist $x \neq 0$ so ist $\psi(x,x) = x\varphi(x)$, so dass in diesem Falle $\varphi(x) = x^{-1}$ ist. Also ist $\psi(x,y) = yx^{-1}$ für alle von Null verschiedenen $x \in K$.

Es sei nun $a \neq 0$. Dann ist $\pi(a, ba) \leq \gamma[b,0]$. Folglich ist

$$\pi\big(a^{-1}, (ba)a^{-1}\big) \leq \gamma[0,b].$$

Hieraus folgt, dass $(ba)a^{-1} = 0a^{-1} + b = b$ ist, q. e. d.

6.12. *Es ist $a(ab) = a^2b$ und $(ba)a = ba^2$ für alle a, $b \in K$, dh., K ist ein* Alternativkörper.

Beweis. Ist $a = 0$, so ist sicherlich $(ba)a = ba^2$. Es gilt

$$0 = 0 \cdot (-1) = (1-1)(-1) = 1 \cdot (-1) + (-1)^2 = -1 + (-1)^2.$$

Also ist $(-1)^2 = 1$.

Weil beide Distributivgesetze gelten, gilt auch $x(-y) = (-x)y = -xy$. Es folgt

$$\big(b(-1)\big)(-1) = -(-b) = b = b(-1)^2.$$

Die Aussage des Satzes gilt also für $a = 0$ und $a = -1$.

Es sei also $a \neq 0$, -1. Dann gilt mit $c \in K$

$$\begin{aligned}\big((ca)(a^{-1} - (a+1)^{-1}\big)(a+1) &= \big(c - (ca)(a+1)^{-1}\big)(a+1) \\ &= ca + c - ca = c.\end{aligned}$$

Hierbei haben wir benutzt, dass $(K,+)$ auf Grund von 6.4 und II.1.15 abelsch ist. Hieraus folgt

$$ca = \big(c(a+1)^{-1}\big)\big(a^{-1} - (a+1)^{-1}\big)^{-1}$$

für alle $c \in K$. Mit $c = a+1$ folgt

$$(a+1)a = (a^{-1} - (a+1)^{-1})^{-1}.$$

Also ist

$$ca = \big(c(a+1)^{-1}\big)\big((a+1)a\big)$$

für alle $c \in K$. Setzt man $c := b(a+1)$, so folgt hieraus

$$(ba)a + ba = b(a^2 + a) = ba^2 + ba$$

und damit $(ba)a = ba^2$. Die andere Identität beweist man entsprechend.

Sind a, b, $c \in K$, so definieren wir den *Assoziator* $[a,b,c]$ durch $[a,b,c] := (ab)c - a(bc)$. Man überzeugt sich leicht, dass der Assoziator in allen Argumenten additiv ist. 6.12 besagt nun gerade, dass $[a,a,b] = 0 = [a,b,b]$ ist. Ferner ist

$$0 = [a, b+c, b+c] = [a,b,b] + [a,b,c] + [a,c,b] + [a,c,c].$$

Also ist $[a, b, c] = -[a, c, b]$. Insbesondere ist also auch $[a, b, a] = 0$. Ebenso leicht rechnet man nach, dass $[a, b, c] = -[b, a, c]$ ist. Dann folgt aber auch $[a, b, c] = -[a, c, b] = [c, a, b] = -[c, b, a]$. Der Assoziator ändert also sein Vorzeichen, wenn man zwei seiner Argumente vertauscht.

Außer dem Assoziator benötigen wir noch den *Kommutator*

$$[a, b] := ab - ba$$

zweier Elemente a, $b \in K$ und die durch

$$k(w, x, y, z) := [wx, y, z] - [x, y, z]w - x[w, y, z]$$

definierte Funktion k. Man überzeugt sich wiederum sehr leicht, dass sowohl der Kommutator als auch die Funktion k in allen Argumenten additiv ist.

6.13. Satz. *Ist ρ eine Permutation von $\{w, x, y, z\}$, so ist*

$$k(w, x, y, z) = \operatorname{sgn}(\rho) k(w^\rho, x^\rho, z^\rho).$$

Beweis. Es ist

$$\begin{aligned}
[wx, y, z] - [xy, z, w] + [yz, w, x] &= [wx, y, z] - [w, xy, z] + [w, x, yz] \\
&= \big((wx)y\big)z - (wx)(yz) - \big(w(xy)\big)z \\
&\quad + w\big((xy)z\big) + (wx)(yz) - \big(w(x(yz)\big) \\
&= [w, x, y]z + w[x, y, z].
\end{aligned}$$

Daher ist

$$\begin{aligned}
&k(w, x, y, z) - k(x, y, z, w) + k(y, z, w, x) \\
&\quad = [wx, y, z] - [x, y, z]w - x[w, y, z] - [xy, z, w] + [y, z, w]x \\
&\qquad + y[x, z, w] + [yz, w, x] - [z, w, x]y - z[y, w, x] \\
&\quad = [w, x, y]z + w[x, y, z] - [x, y, z]w - x[w, y, z] + [y, z, w]x \\
&\qquad + y[x, z, w] - [z, w, x]y - z[y, w, x] \\
&\quad = \big[w, [x, y, z]\big] + \big[[w, x, y], z\big] + \big[[y, z, w], x\big] + \big[y, [x, z, w]\big].
\end{aligned}$$

Es ist also

$$\begin{aligned}
&k(w, x, y, z) - k(x, y, z, w) + k(y, z, w, x) \\
&\quad = \big[w, [x, y, z]\big] + \big[[w, x, y], z\big] + \big[[y, z, w], x\big] + \big[y, [x, z, w]\big].
\end{aligned}$$

Ersetzt man hierin w, x, y, z durch x, y, z, w, so erhält man

$$\begin{aligned}
&k(x, y, z, w) - k(y, z, w, x) + k(z, w, x, y) \\
&\quad = \big[x, [y, z, w]\big] + \big[[x, y, z], w\big] + \big[[z, w, x], y\big] + \big[z, [y, w, x]\big].
\end{aligned}$$

Addiert man diese beiden Gleichungen, so ergibt sich

$$k(w, x, y, z) + k(z, w, x, y) = 0.$$

Also ist

$$k(w,x,y,z) = -k(z,w,x,y).$$

Ferner ist

$$\begin{aligned} k(w,x,y,z) &= [wx,y,z] - [x,y,z]w - x[w,y,z] \\ &= -\big([wx,z,y] - [x,z,y]w - x[w,z,y]\big) \\ &= -k(w,x,z,y). \end{aligned}$$

Definiert man σ durch $w^\sigma := z$, $x^\sigma := w$, $y^\sigma := x$, $z^\sigma := y$ und τ durch $w^\tau := w$, $x^\tau := x$, $y^\tau := z$ und $z^\tau := y$, so ist σ ein 4-Zyklus und τ eine Transposition, daher ist $\mathrm{sgn}(\sigma) = -1 = \mathrm{sgn}(\tau)$. Also ist

$$k(w,x,y,z) = \mathrm{sgn}(\sigma)k(w^\sigma,x^\sigma,y^\sigma,z^\sigma) = \mathrm{sgn}(\tau)k(w^\tau,x^\tau,y^\tau,z^\tau).$$

Weil σ und τ die symmetrische Gruppe auf $\{x,y,z,w\}$ erzeugen, folgt damit die Behauptung von 6.13.

Nun ist $k(w,x,y,y) = 0$. Aus 6.13 folgt, dass sicher dann $k(w,x,y,z) = 0$ ist, falls zwei der Argumente gleich sind.

Der nächste Satz ist der Schlüssel zum Beweise des Satzes von Artin-Zorn, dass nämlich endliche Alternativkörper Körper sind. Dabei spielt auch eine Rolle, dass die multiplikative Gruppe eines endlichen Körpers zyklisch ist, so dass endliche Körper von einem Element erzeugt werden.

Alternativkörper beschreiben stets Moufangebenen. Das werden wir hier nicht beweisen, da es zum Beweise von 6.14 und dem Satz von Artin-Zorn nicht benötigt wird. Der interessierte Leser sei für die Theorie der Alternativkörper auf Pickert 1955, Kapitel 6 verwiesen.

6.14. Satz. *Sind a und b Elemente des Alternativkörpers K, so gibt es einen assoziativen Unterring von K, der a und b enthält.*

Beweis. Wir setzen $E := \{a,b\}$. Sind e, f, $g \in E$, so ist $[e,f,g] = 0$, da wenigstens zwei der Elemente e, f, g gleich sind. Wir definieren die Menge X durch

$$X := \{x \mid x \in K,\ [e,f,x] = 0 \text{ für alle } e,f \in E\}.$$

Dann ist $E \subseteq X$, wie wir gerade gesehen haben. Sind e, f, $g \in E$ und ist $x \in E$, so ist

$$[ex,f,g] = k(e,x,f,g) + [x,f,g]e + x[e,f,g] = 0,$$

auf Grund der Definition von X bzw. der Tatsache, dass zwei der Elemente e, f, g gleich sind. Also ist $EX \subseteq X$. Wir definieren Y durch

$$Y := \big\{y \mid y \in K, [e,x,y] = 0 \text{ für alle } e \in E \text{ und alle } x \in X\big\}.$$

Wegen $E \subseteq X$ ist $Y \subseteq X$. Es sei $y \in Y$ und $x \in X$ und e, $f \in E$. Dann ist

$$\begin{aligned} [e,f,yx] &= [yx,e,f] \\ &= k(y,x,e,f) + [x,e,f]y + x[e,y,f] \\ &= k(y,x,e,f) = -k(e,x,y,f) \\ &= -[ex,y,f] + [x,y,f]e + x[e,y,f] = 0, \end{aligned}$$

da auf Grund der Definition von Y und wegen $EX \subseteq X$ die Assoziatoren $[ex, y, f]$, $[x, y, f]$ und $[e, y, f]$ alle gleich Null sind. Somit ist auch $YX \subseteq X$. Schließlich sei

$$R := \big\{ r \mid r \in K, [x, y, r] = 0 \text{ für alle } x \in X \text{ und alle } y \in Y \big\}.$$

Aus der Definition von X und Y folgt $E \subseteq R$. Weil $E \subseteq Y$ ist, ist $R \subseteq Y$. Also ist $E \subseteq R \subseteq Y \subseteq X$. Folglich ist $[r, s, t] = 0$ für alle r, s, $t \in R$. Weil R wegen $E \subseteq R$ nicht leer ist und offensichtlich $r - s \in R$ gilt für alle r, $s \in R$, ist $(R, +)$ eine Gruppe. Es seien r, $s \in R$ und $x \in X$ und $y \in Y$. Dann ist

$$k(x, y, r, s) = [yx, r, r] - [x, r, s]y - x[y, r, s] = 0,$$

da $R \subseteq Y$ und $YX \subseteq X$ ist. Nach 6.13 ist folglich auch $k(r, s, y, x) = 0$. Somit ist

$$0 = [rs, y, x] - [s, x, y]r - s[r, y, x] = [rs, y, x].$$

Also ist auch $rs \in R$, so dass R in der Tat ein assoziativer Ring ist, der a und b enthält.

6.15. Satz von Artin-Zorn. *Ist K ein endlicher Alternativkörper, so ist K ein Körper.*

Beweis. Es sei S ein maximaler assoziativer Teilring von K. Weil K endlich ist und keine Nullteiler hat, folgt, dass S ein endlicher, nullteilerfreier Ring ist. Folglich ist S ein Körper. Als endlicher Körper ist S nach dem Satz von Wedderburn kommutativ. Insbesondere ist die multiplikative Gruppe von S zyklisch. Es sei a ein erzeugendes Element der multiplikativen Gruppe von S. Es sei $b \in K$. Nach 6.14 gibt es einen assoziativen Teilring R von K mit $a, b \in R$. Es folgt $S \subseteq R$ und damit $S = R$, da S ja ein maximaler assoziativer Teilring von K ist. Also ist $b \in S$ und somit $K = S$, so dass K in der Tat ein Körper ist.

Wir sind nun in der Lage, Satz 6.1 zu beweisen. Weil M endlich ist, ist K nach 6.15 ein Körper. Es sei $k \in K^*$. Wir definieren $\sigma(k)$ durch

$$\pi(x, y)^{\sigma(k)} := \pi(xk, yk).$$

Dann ist $\sigma(k)$ eine Bijektion der Punktmenge von M_{UV} auf sich und es gilt $\sigma(k)^{-1} = \sigma(k^{-1})$. Ferner folgt aus $\pi(c, y)^{\sigma(k)} = \pi(ck, yk)$ und

$$\pi(x, mx + b)^{\sigma(k)} = \pi\big(xk, (mx + b)k\big) = \pi\big(xk, m(xk) + b\big),$$

dass $\sigma(k)$ kollineare Punkte auf kollineare Punkte abbildet. Weil dann auch $\sigma(k^{-1})$ kollineare Punkte auf kollineare Punkte abbildet, ist $\sigma(k)$ eine Kollineation von M_{UV}. Weil $\sigma(k)$ offensichtlich jede Gerade auf eine zu ihr parallele Gerade abbildet und weil $O^{\sigma(k)} = O$ ist, ist $\sigma(k) \in \Delta(O, UV)$. Aus

$$E^{\sigma(k)} = \pi(1, 1)^{\sigma(k)} = \pi(k, k)$$

folgt schließlich, dass M eine (O, UV)-transitive Ebene ist. Da dies für alle nicht kollinearen Punkte O, U, V gilt, ist M nach II.1.8 desarguessch.

7. Ebenen mit vielen Perspektivitäten

Ist K eine Kollineationsgruppe eines projektiven Verbandes L und ist H eine Hyperebene von L, so setzen wir $K(H) := K \cap \mathrm{E}(H)$. Ist außerdem P ein Punkt von L, so setzen wir $K(P,H) := K \cap \Delta(P,H)$. Es ist also $K(H)$ die Menge der in K enthaltenen Elationen mit der Achse H und $K(P,H)$ die Menge der in K enthaltenen Perspektivitäten mit der Achse H und dem Zentrum P. Sowohl $K(H)$ als auch $K(P,H)$ sind Untergruppen von K. Der Leser beachte, dass $K(H)$ immer eine Gruppe von Elationen ist, während $K(P,H)$ auch eine Gruppe von Streckungen sein kann.

7.1. Satz. *Es sei L ein endlicher projektiver Verband mit* $\mathrm{Rg}(L) \geq 3$ *und K sei eine Kollineationsgruppe von L. Ist H eine Hyperebene von L und ist B die Menge der Punkte von L_H mit $K(P,H) \neq \{1\}$, so ist B eine Bahn von $K(H)$.*

Beweis. Es sei Γ die Menge aller in K enthaltenen Perspektivitäten mit der Achse H. Dann ist Γ eine Untergruppe von K. Setze $a_P := |K(P,H)|$. Dann ist

$$|\Gamma| = \big|K(H)\big| + \sum_{P \in B} (a_P - 1),$$

da ja jedes von 1 verschiedene Elemente von Γ genau ein Zentrum hat. Setze $k := |B|$. Weil $|K(H)| \geq 1$ und $a_P \geq 2$ ist, ist $|\Gamma| \geq 1 + k > k$. Es seien $B_1, \ldots, B_r$, die Punktbahnen von Γ mit $|B_i| < |\Gamma|$. Dann ist $B = \bigcup_{i:=1}^r B_i$. Ist $P \in B_i$, so ist $|\Gamma| = |B_i||K(P,H)|$. Also ist

$$\begin{aligned}
|\Gamma| &= \big|K(H)\big| - k + \sum_{P \in B} \big|K(P,H)\big| \\
&= \big|K(H)\big| - k + \sum_{i:=1}^{r} \sum_{P \in B_i} \big|K(P,H)\big| \\
&= \big|K(H)\big| - k + \sum_{i:=1}^{r} \sum_{P \in B_i} |\Gamma||B_i|^{-1} \\
&= \big|K(H)\big| - k + \sum_{i:=1}^{r} |\Gamma|. \\
&= \big|K(H)\big| - k + r|\Gamma|.
\end{aligned}$$

Folglich ist

$$0 \leq (r-1)|\Gamma| = k - \big|K(H)\big| < k < |\Gamma|.$$

Hieraus folgt, dass $0 \leq r - 1 < 1$ ist. Dies impliziert wiederum $r = 1$ und dann $k = |K(H)|$.

$K(H)$ zerlegt B in Bahnen. Weil $K(H)$ auf der Menge der Punkte von L_H regulär operiert, folgt aus $|K(H) = k = |B|$, dass B eine Bahn von $K(H)$ ist. Damit ist der Satz bewiesen.

7.2. Korollar. *Es sei L ein endlicher projektiver Verband, dessen Rang mindestens* 3 *sei. Sind dann ρ und σ von* 1 *verschiedene Streckungen von L mit*

den Zentren P und Q und haben ρ und σ die gleiche Achse H, so gibt es in der von ρ und σ erzeugten Gruppe eine Elation τ, die natürlich ebenfalls die Achse H hat, mit $P^\tau = Q$.

Dies folgt unmittelbar aus 7.1.

7.3. Satz. *Es sei E eine endliche projektive Ebene. Ist K eine Kollineationsgruppe von E und ist $K(P,G) \neq \{1\}$ für alle nicht inzidenten Punkt-Geradenpaare (P,G) von E, so ist E desarguessch und K enthält die kleine projektive Gruppe von E.*

Beweis. Ist G eine Gerade von E, so ist $K(G)$ nach 7.1 auf der Menge der Punkte von E_G transitiv. Dies besagt einmal, dass E eine Moufangebene und somit nach 6.1 desarguessch ist, und zum anderen, dass K alle Elationen von E und folglich die kleine projektive Gruppe von E enthält.

Der Satz, dass eine Korrelation eines endliche projektiven Verbandes stets einen absoluten Punkt hat, hat eine überraschende Konsequenz, nämlich den folgenden Satz.

7.4. Satz. *Es sei L ein endlicher projektiver Verband mit* $\mathrm{Rg}(L) \geq 3$*. Ist K eine Kollineationsgruppe von L und ist jeder Punkt von L Zentrum einer nicht trivialen Streckung aus K, so enthält K eine nicht triviale Elation.*

Beweis. Ist L ein Gegenbeispiel zu 7.4, so folgt aus dem zu 7.2 dualen Satz, dass es zu jedem Punkt P von L genau eine Hyperebene P^π gibt mit $P \notin P^\pi$ und $K(P,P^\pi) \neq \{1\}$. Aus 7.2 folgt ferner, dass π injektiv ist. I.7.7 impliziert schließlich, dass π eine Bijektion der Menge der Punkte auf die Menge der Hyperebenen von L ist.

Es sei $r := \mathrm{Rg}(L)$. Wir zeigen als Nächstes, dass das Abbildungspaar $\kappa := (\pi, \pi^{-1})$ eine Korrelation von $L_{1,r-1}$ ist. Es sei P ein Punkt und H eine Hyperebene von L. Ferner sei $Q := H^{\pi^{-1}}$. Ist $P \leq H$, so folgt $H^\sigma = H$ für alle $\sigma \in K(P,P^\pi)$. Hieraus folgt wiederum, dass $Q^\sigma = Q$ ist für alle $\sigma \in K(P,P^\pi)$. Wegen $Q \notin Q^\pi = H$ und $P \leq H$ ist $Q \neq P$. Daher ist $Q \leq P^\pi$ nach II.1.3. Damit ist gezeigt, dass $Q \leq P^\pi$ aus $P \leq H = Q^\pi$ folgt. Wegen $\kappa^2 = 1$ gilt daher $P \leq Q^\pi$ genau dann, wenn $Q \leq P^\pi$ ist. Damit ist κ als Korrelation von $L_{1,r-1}$ erkannt. Da κ eine Korrelation von $L_{1,r-1}$ ist, gibt es nach 4.3a) einen Punkt W mit $W \leq W^\kappa$. Andererseits ist $P \not\leq P^\pi$ für alle Punkte P von L, ein Widerspruch.

7.5. Satz *Es sei E eine endlich projektive Ebene und K eine Kollineationsgruppe von E. Ist (P,G) eine Fahne von E, so ist entweder $|K(P,G)|^2 \geq |K(G)|$ oder alle Elationen aus K, deren Zentrum P ist, haben G als Achse.*

Beweis. Es sei H eine von G verschiedene Gerade durch P und es sei $1 \neq \tau \in K(P,H)$. Ist $\sigma \in K(G)$, so ist $\sigma^{-1}\tau\sigma \in K(P,H^\sigma)$. Folglich hat $\tau^{-1}\sigma^{-1}\tau\sigma$ das Zentrum P. Andererseits ist $\tau^{-1}\sigma^{-1}\tau \in K(G^\tau) = K(G)$. Daher hat $\tau^{-1}\sigma^{-1}\tau\sigma$ die Achse G. Also ist

$$\tau^{-1}\sigma^{-1}\tau\sigma \in K(P,G).$$

Es sei $\rho \in K(G)$. Genau dann ist $\tau^{-1}\sigma^{-1}\tau\sigma = \tau^{-1}\rho^{-1}\tau\rho$, wenn $\rho\sigma^{-1}\tau = \tau\rho\sigma^{-1}$ ist. Wegen $\tau \neq 1$ ist dies genau dann der Fall, wenn $H^{\rho\sigma^{-1}} = H$ ist, dh., wenn

$\rho\sigma^{-1} \in K(P,G)$ ist. Es gibt somit genau $|K : K(P,G)|$ Elemente der Form $\tau^{-1}\sigma^{-1}\tau\sigma$. Da alle diese Elemente in $K(P,G)$ liegen, ist $|K(P,G)| \geq |K(G) : K(P,G)|$, q. e. d.

7.6. Satz. *Es sei E eine endliche projektive Ebene der Ordnung n. Ist G eine Gerade von E und K eine Kollineationsgruppe mit $|K(G)| > n$, so hat $K(G)$ eine Geradenbahn der Länge n. Insbesondere ist n Teiler von $|K(G)|$.*

Beweis. Es sei H eine Gerade von E mit der Eigenschaft, dass die Länge a der Bahn, zu der H gehört, maximal sei. Ist t die Anzahl der Punktbahnen von $K(G)$ in E_G, so folgt, da K nach 3.4 in E ebenso viele Punkt- wie Geradenbahnen hat, dass $K(G)$ in E_G genau $t+n$ Geradenbahnen hat, da $K(G)$ ja alle Punkte von G festlässt und folglich in E genau $t+n+1$ Punktbahnen hat. Nun ist $n(n+1)$ die Anzahl der von G verschiedenen Geraden von E. Daher folgt aus der Maximalität von a, dass $a(t+n) \geq n(n+1)$ ist. Andererseits ist $n^2 = t|K(G)| \geq tn$, so dass $t \leq n$ ist. Hieraus folgen die Ungleichungen

$$2an = a(n+n) \geq a(t+n) \geq n(n+1)$$

und somit $2a \geq n+1 > n$. Ist $P := G \cap H$ und ist L eine von G verschiedene Gerade durch P, so ist $K(G)_L = K(P,G) = K(G)_H$. Folglich ist

$$\big|K(G) : K(G)_L\big| = \big|K(G) : K(G)_H\big| = a.$$

Daher wird die Menge der n von G verschiedenen Geraden durch P in lauter Bahnen der Länge a zerlegt, so dass a Teiler von n ist. Weil aber $2a > n$ gilt, kann dies nur so sein, dass $a = n$ ist. Damit ist der Satz bewiesen.

7.7. Satz. *Es sei E eine endliche projektive Ebene der Ordnung n und K sei eine Kollineationsgruppe von E. Ist G eine Gerade von E und ist $|K(G)| \geq n+1$, so ist $K(P,G) \neq \{1\}$ für alle Punkte P auf G. Überdies ist n Potenz einer Primzahl.*

Beweis. Es sei P ein Punkt auf G und H sei eine von G verschiedene Gerade durch P. Ist a die Länge der Bahn von H unter $K(G)$, so ist wegen $K(G)_H = K(P,G)$ dann

$$n\big|K(P,G)\big| \geq a\big|K(P,G)\big| = \big|K(G)\big| \geq n+1.$$

Hieraus folgt $K(P,G) \neq \{1\}$.

Weil $K(P,G) \neq \{1\}$ ist für alle $P \leq G$ ist $K(G)$ nach II.1.13 eine elementarabelsche p-Gruppe. Schließlich ist n wegen $|K(G)| \geq n+1$ nach 7.6 ein Teiler von $|K(G)|$, so dass also auch n eine Potenz von p ist. Damit ist alles bewiesen.

7.8. Satz. *Es sei E eine projektive Ebene der Ordnung n. Ferner sei (P,G) eine Fahne und K eine Kollineationsgruppe von E. Ist dann h eine natürliche Zahl mit $h > 1$ und ist $|K(Q,G)| = h$ für alle von P verschiedenen Punkte Q auf G, so ist $|K(P,G)| = n$.*

Beweis. Es ist

$$\big|K(G)\big| = \big|K(P,G)\big| + n(h-1).$$

Aus $h > 1$ folgt $|K(G)| \geq n + 1$. Aus 7.6 erschließen wir daher, dass n Teiler von $|K(G)|$ ist. Dann ist n aber auch Teiler von $|K(P,G)|$. Hieraus folgt zusammen mit den trivialerweise geltenden Ungleichungen $1 \leq |K(P,G)| \leq n$ die Behauptung.

Eine unmittelbare Folgerung aus 7.8 ist

7.9. Korollar. *Es sei E eine endliche projektive Ebene der Ordnung n und G sei eine Gerade von E. Ist K eine Kollineationsgruppe von E und ist $h > 1$ eine natürliche Zahl, ist ferner $|K(P,G)| = h$ für alle Punkte P auf G, so ist $h = n$ und E ist eine Translationsebene bez. G. Außerdem enthält K alle Elationen mit der Achse G.*

7.10. Satz. *Es sei Ω eine endliche Menge und Δ sei eine Teilmenge von Ω. Ferner sei G eine Permutationsgruppe auf Ω und p sei eine Primzahl. Gibt es dann zu jedem $\delta \in \Delta$ eine p-Untergruppe $G(\delta)$ von G_δ, die außer δ kein weiteres Fixelement hat, so ist Δ in einer Bahn von G enthalten.*

Beweis. Es sei $\delta \in \Delta$ und Σ sei die Bahn von δ unter G. Dann wird Σ von $G(\delta)$ in Bahnen $\Sigma_1 = \{\delta\}$, $\Sigma_2, \ldots, \Sigma_t$ zerlegt. Auf Grund unserer Annahme ist $|\Sigma_i| > 1$ für alle $i \geq 2$. Weil $G(\delta)$ eine p-Gruppe ist, ist daher $|\Sigma_i|$ als Teiler von $|G(\delta)|$ durch p teilbar. Daher ist

$$|\Sigma| = \sum_{i:=1}^{t} |\Sigma_i| \equiv |\sigma_1| \equiv 1 \bmod p.$$

Es sei $\eta \in \Delta$ und $\eta \notin \Sigma$. Die Gruppe $G(\eta)$ zerlegt Σ in Bahnen $\Sigma'_1, \ldots, \Sigma'_s$. Weil $\eta \notin \Sigma$ ist, folgt $|\Sigma'_i| > 1$ und damit $|\Sigma'_i| \equiv 0 \bmod p$ für alle i. Hiermit erhalten wir den Widerspruch

$$|\Sigma| = \sum_{i:=1}^{t} |\Sigma'_i| \equiv 0 \bmod p.$$

Dieser Widerspruch zeigt, dass doch $\Delta \subseteq \Sigma$ ist.

7.11. Satz. *Es sei E eine endliche projektive Ebene und K sei eine Kollineationsgruppe von E. Ist dann jeder Punkt von E Zentrum und jede Gerade von E Achse einer nicht trivialen Elation aus K, so ist E desarguessch und K enthält die kleine projektive Gruppe von E.*

Beweis. Wir zeigen zunächst, dass $K(P,G) \neq \{1\}$ ist für alle Fahnen (P,G) von E. Angenommen es sei (P,G) eine Fahne mit $K(P,G) = \{1\}$. Auf Grund unserer Annahme ist $K(G) \neq \{1\}$ und $K(P,H) \neq \{1\}$ für wenigstens eine von G verschiedene Gerade H durch P. Mit 7.5 erhalten wir daher den Widerspruch

$$1 = \big|K(P,G)\big|^2 \geq \big|K(G)\big| > 1.$$

Also ist doch $K(P,G) \neq \{1\}$.

Es sei n die Ordnung von E. Wegen $K(P,G) \neq \{1\}$ ist $|K(G)| > n + 1$, so dass n nach 7.7 Potenz einer Primzahl ist. Überdies ist n nach 7.6 Teiler von

$|K(G)|$. Nach II.1.15 ist $K(G)$ eine elementarabelsche p-Gruppe. Da n auch ein Teiler von $|K(H)|$ ist, wenn H eine Gerade von E ist, so folgt, dass $K(H)$ für alle Geraden H von E eine elementarabelsche p-Gruppe ist.

Es sei weiterhin G eine Gerade von E. Ist P ein Punkt auf G und ist H eine von G verschiedene Gerade durch P, so ist $K(P,H)$ eine p-Gruppe, die auf G eine Permutationsgruppe induziert, die P und nur P zum Fixpunkt hat. Mit 7.10 folgt daher, dass der Stabilisator K_G von G in K auf der Menge der Punkte von G transitiv operiert. Hieraus folgt wiederum, dass die Gruppen $K(P,G)$ mit $P \leq G$ alle in K konjugiert sind und folglich alle die Ordnung $h > 1$ haben. 7.9 impliziert nun, dass E eine Translationsebene bez. G ist und dass $\mathrm{E}(G)$ in K enthalten ist. Somit ist E eine Moufangebene und daher nach 6.1 desarguessch. Überdies enthält K die kleine projektive Gruppe von E.

7.12. Korollar. *Es sei E eine endliche projektive Ebene und K sei eine auf der Menge der Punkte von E transitive Kollineationsgruppe von E. Enthält K eine von* 1 *verschiedene Perspektivität, so ist E desarguessch und K enthält die kleine projektive Gruppe.*

Beweis. Enthält K eine nicht triviale Streckung, so folgt aus der Punkttransitivität von K, dass jeder Punkt von E Zentrum einer nicht trivialen Streckung aus K ist. Nach 7.4 enthält K dann auch eine nicht triviale Elation, so dass wir von vornherein annehmen dürfen, dass K eine nicht triviale Elation enthält. Wir folgern wiederum aus der Punktransitivität von K, dass jeder Punkt von E Zentrum einer nicht trivialen Elation aus K ist. Weil K nach 3.4 auch auf der Menge der Geraden von E transitiv ist, ist auch jede Gerade von E Achse einer nicht trivialen Elation aus K. Anwendung von 7.11 liefert nun die Behauptung.

8. Einiges über Permutationsgruppen

In diesem Abschnitt beweisen wir einige Sätze über Permutationsgruppen, die wir im nächsten Abschnitt benötigen werden.

8.1. Satz. *Es sei Γ eine Permutationsgruppe auf der Menge M und B und C seien zwei Bahnen von Γ mit $\mathrm{ggT}(|B|,|C|) = 1$. Ist $b \in B$, so ist C auch eine Bahn von Γ_b.*

Beweis. Es sei $c \in C$ und C' sei die Bahn von c unter Γ_b. Ferner sei B' die Bahn von b unter Γ_c. Dann ist

$$|\Gamma| = |B||\Gamma_b| = |B||C'||\Gamma_{b,c}|$$

und

$$|\Gamma| = |C||\Gamma_c| = |C||B'||\Gamma_{c,b}|.$$

Wegen $\Gamma_{b,c} = \Gamma_{c,b}$ ist $|B||C'| = |C||B'|$. Weil $|B|$ und $|C|$ teilerfremd sind, folgt, dass $|C|$ Teiler von $|C'|$ ist. Weil andererseits C' in C enthalten ist, folgt $C = C'$, q. e. d.

8.2. Satz. *Es sei Γ eine auf der Menge M transitiv operierende Permutationsgruppe. Ferner sei $n := |M|$ endlich und p sei eine in $|\Gamma|$ aufgehende Primzahl.*

Schließlich sei p^a mit $a \geq 0$ die höchste Potenz von p, die in n aufgeht. Ist Π eine p-Sylowgruppe von Γ, so ist die Länge einer jeden Bahn von Π durch p^a teilbar. Insbesondere ist die Länge jeder kürzesten Bahn von Π gleich p^a.

Beweis. Es sei $x \in M$ und p^b sei die höchste in $|\Gamma_x|$ aufgehende Potenz von p. Dann ist $|\Pi| = p^{a+b}$. Es sei B eine Bahn von Π. Dann ist

$$p^{a+b} = |\Pi| = |B||\Pi_y|,$$

wobei $y \in B$ ist. Wegen $\Pi_y \subseteq \Gamma_y$ und $|\Gamma_y| = |\Gamma_x|$, letzteres weil die beiden Gruppen wegen der Transitivität von Γ konjugiert sind, ist $|\Pi_y|$ Teiler von p^b. Somit ist $|B|$ durch p^a teilbar.

Sind $B_1, \ldots, B_r$ alle Bahnen von Π, so ist $n = \sum_{i:=1}^{r} |B_i|$. Weil n nicht durch p^{a+1} teilbar ist, können nicht alle $|B_i|$ durch p^{a+1} teilbar sein. Folglich hat Π eine Bahn der Länge p^a.

Der nächste Satz ist einer der ältesten Sätze aus der Theorie der Permutationsgruppen. Er stammt von Evariste Galois.

8.3. Satz. *Es sei Γ eine auf M primitiv operierende endliche Permutationsgruppe. Enthält Γ einen von $\{1\}$ verschiedenen, auflösbaren Normalteiler, so enthält Γ einen und nur einen minimalen Normalteiler N. Der Normalteiler N ist eine elementarabelsche p-Gruppe und es ist $|N| = |M|$.*

Beweis. Γ enthält einen nicht trivialen auflösbaren Normalteiler B. Es gibt daher eine natürliche Zahl i mit $N := B^{(i)} \neq \{1\}$ und $B^{(i+1)} = \{1\}$. Weil N in B charakteristisch ist, ist N in Γ normal. Weil Γ auf M primitiv operiert, ist N folglich transitiv auf M. Überdies ist N abelsch, da ja $N' = B^{(i+1)} = \{1\}$ ist. Hieraus folgt weiter, dass N auf M scharf transitiv operiert, so dass $|M| = |N|$ ist. Dies impliziert, dass N ein minimaler Normalteiler ist. Folglich ist N charakteristisch einfach und als abelsche Gruppe dann eine elementarabelsche p-Gruppe.

Es sei N^* ein von N verschiedener minimaler Normalteiler. Dann ist $N^* \cap N = \{1\}$ und folglich $N^* \subseteq C_\Gamma(N) = N$. Dieser Widerspruch beweist die Einzigkeit von N. Damit ist alles bewiesen.

8.4. Satz. *Es sei n eine ungerade natürliche Zahl und Γ sei eine Permutationsgruppe der Ordnung $2n$, die auf der Menge M der Länge n transitiv operiere. Ist der Stabilisator irgend zweier Elemente von M in Γ stets trivial, so gilt:*

a) *Sind a und b zwei verschiedene Elemente von M, so gibt es eine Involution in Γ, welche a und b vertauscht.*
b) *Ist Δ eine Untergruppe von Γ, die genau $r \geq 1$ Involutionen enthält, so ist $|\Delta| = 2r$.*

Beweis. Da n ungerade ist und weil der Stabilisator zweier verschiedener Elemente von M in Γ stets trivial ist, hat jede Involution aus Γ genau einen Fixpunkt. Wegen $|\Gamma_x| = 2$ für alle $x \in M$ enthält Γ daher genau n Involutionen. Sind γ und δ zwei Involutionen aus Γ und ist $a^\gamma = a^\delta$ für ein $a \in M$, so ist $\gamma = \delta$. Ist nämlich $a = a^\gamma = a^\delta$, so ist $\gamma, \delta \in \Gamma_a$ und aus $|\Gamma_a| = 2$ folgt $\gamma = \delta$. Ist $a \neq a^\gamma$, so folgt $a^{\gamma\delta} = a^{\delta^2} = a$ und $(a^\gamma)^{\gamma\delta} = a^\delta = a^\gamma$. Somit lässt $\gamma\delta$ sowohl

a als auch a^γ fest. Nach Voraussetzung ist daher $\gamma\delta = 1$ und folglich $\gamma = \delta$. Hieraus folgt

$$\bigl|\{a^\gamma \mid \gamma \text{ ist Involution aus } \Gamma\}\bigr| = n.$$

Daher ist

$$M = \{a^\gamma \mid \gamma \text{ ist Involution aus } \Gamma\},$$

so dass es in der Tat eine Involution gibt, die a mit b vertauscht.

Es sei δ eine Involution aus Δ und a sei der Fixpunkt von Δ. Mit T bezeichnen wir die Bahn von a unter Δ. Dann ist $|\Delta| = |T||\Delta_a|$. Wegen $1 < |\Delta_a| \leq |\Gamma_a| = 2$ ist daher $|\Delta| = 2|T|$. Nun hat δ keinen Fixpunkt in $T - \{a\}$, so dass $|T|$ ungerade ist. Das Paar (Δ, T) erfüllt somit ebenfalls die Voraussetzungen von 8.4. Wie der Beweis von a) zeigt, enthält Δ daher genau $|T|$ Involutionen, so dass also $|T| = r$ ist. Damit ist der Satz bewiesen.

8.5. Satz. *Es sei M eine Menge mit $n+1$ Elementen und n sei ungerade. Ferner sei Γ eine auf M zweifach transitive Permutationsgruppe. Ist $a \in M$ und enthält Γ_a eine Untergruppe F_a gerader Ordnung, die auf $M - \{a\}$ transitiv operiert und die ferner die Eigenschaft hat, dass $F_{a,b,c} = \{1\}$ ist für alle b, $c \in M - \{a\}$ mit $b \neq c$, so operiert Γ_a auf $M - \{a\}$ primitiv.*

Beweis. F_a operiert als Frobeniusgruppe auf $M - \{a\}$. Daher besitzt F_a eine charakteristische Untergruppe K_a, den Frobeniuskern von F_a, die auf $M - \{a\}$ scharf transitiv operiert (siehe etwa Huppert 1967, Satz 8.2, S. 496). Es gibt ferner eine Involution $\gamma \in F_a$, da die Ordnung von F_a gerade ist. Wegen $|K_a| = n \equiv 1 \bmod 2$ ist $\gamma \in K_a$. Folglich ist $K_a\langle\gamma\rangle$ eine Untergruppe der Ordnung $2n$, die ebenfalls als Frobeniusgruppe auf $M - \{a\}$ operiert. Wir dürfen daher annehmen, dass $|F_a| = 2n$ ist. Aufgrund der Transitivität von Γ auf M enthält dann Γ_b für alle $b \in M$ eine solche Frobeniusgruppe F_b.

Wir nehmen nun an, dass Γ_a auf $M - \{a\}$ imprimitiv operiert. Es sei $I := \{a_1, \ldots, a_t\}$ ein Imprimitivitätsgebiet von Γ_a. Dann ist $1 < t < n$. Ferner ist t Teiler von n, so dass t insbesondere ungerade ist. Wir setzen $T := I \cup \{a\}$. Es sei $b \in M - T$. Nach 8.4a) gibt es für $i := 1, \ldots, t$ eine Involution $\gamma_i \in F_b$ mit $a^{\gamma_i} = a_i$. Wir zeigen, dass $T^{\gamma_i} = T$ ist. Offensichtlich ist $a^{\gamma_i} \in T$. Es sei $c := a_j^{\gamma_i} \notin T$. Dann ist $j \neq i$ da andernfalls $c = a \in T$ wäre. Wiederum nach 8.4a) gibt es eine Involution $\gamma \in F_c$ mit $a^\gamma = a_i$. Hieraus folgt, $a^{\gamma_i\gamma} = a_i^\gamma = a$ und somit $\gamma_i\gamma \in \Gamma_a$. Ferner ist $a_i^{\gamma_i\gamma} = a^\gamma = a_i$. Folglich ist $I^{\gamma_i\gamma} \cap I \neq \emptyset$ und daher $I^{\gamma_i\gamma} = I$. Hieraus folgt $c = c^\gamma = a_j^{\gamma_i\gamma} \in I$ und damit der Widerspruch $c \in T$. Dieser Widerspruch zeigt, dass $T^{\gamma_i} \subseteq T$ und damit, dass $T^{\gamma_i} = T$ ist.

Wir betrachten nun die Gruppe $\Delta := \langle\gamma_i \mid i := 1, \ldots, t\rangle$. Dann ist Δ eine Untergruppe von F_b, die auf T transitiv operiert. Weil $|T| = t + 1$ gerade ist, muss Δ als Untergruppe von F_b scharf transitiv operieren. Also ist $|\Delta| = t + 1$. Andererseits enthält T mindestens t Involutionen. Nach 8.4b) ist daher $|\Delta| \geq 2t$. Folglich ist $t + 1 \geq 2t$, woraus der Widerspruch $t = 1$ folgt. Damit ist der Satz bewiesen.

8.6. Satz. *Die Voraussetzungen seien die gleichen wie in 8.5. Ist der Frobeniuskern K_a von F_a normal in Γ_a, so ist K_a eine elementarabelsche p-Gruppe und n ist eine Potenz von p.*

Beweis. Auf Grund von 8.5 und 8.3 genügt es zu zeigen, dass K_a abelsch ist. Wie wir wissen, gibt es eine Involution $\sigma \in \Gamma_a$, die genau einen Fixpunkt $b \in M - \{a\}$ hat. Weil K_a in Γ_a normal ist, ist $K_a^\sigma = K_a$. Es sei $\kappa \in K_a$ und $\kappa^\sigma = \kappa$. Dann ist σ mit κ vertauschbar und folglich $b^\kappa = b$, woraus $\kappa = 1$ folgt. Ist $\kappa^\sigma \kappa^{-1} = \lambda^\sigma \lambda^{-1}$ mit κ, $\lambda \in K_a$, so ist $(\lambda^{-1}\kappa)^\sigma = \lambda^{-1}\kappa$ und daher $\kappa = \lambda$. Also ist

$$\bigl|\{\kappa^\sigma \kappa^{-1} \mid \kappa \in K_a\}\bigr| = n,$$

so dass

$$K_a = \{\kappa^\sigma \kappa^{-1} \mid \kappa \in K_a\}$$

ist. Es sei nun $\lambda \in K_a$. Dann gibt es also ein $\kappa \in K_a$ mit $\lambda = \kappa^\sigma \kappa^{-1}$. Daher ist

$$\lambda^\sigma = \kappa^{\sigma^2} \kappa^{-\sigma} = \kappa \kappa^{-\sigma} = (\kappa^\sigma \kappa^{-1})^{-1} = \lambda^{-1}.$$

Da dies für alle $\lambda \in K_a$ gilt, folgt, dass K_a abelsch ist.

9. Geradenhomogene affine Ebenen

Hauptziel dieses Abschnitts ist zu zeigen, dass eine endliche affine Ebene, deren Kollineationsgruppe die Geraden transitiv permutiert, eine Translationsebene ist. Um dies zu beweisen, benötigen wir noch einige Hilfsmittel, die wir zuvor bereitstellen.

9.1. Satz. *Ist E eine projektive Ebene und ist γ eine involutorische Kollineation von E, so gilt eine der beiden folgenden Aussagen:*
a) *γ ist eine Perspektivität von E.*
b) *Die aus den Fixpunkten und Fixgeraden von γ bestehende Teilstruktur von E ist eine projektive Ebene F. Jede Gerade von E trägt einen Punkt von F und jeder Punkt von E liegt auf einer Geraden von F.*

Beweis. Wir führen den Beweis in mehreren Schritten.
1) Ist P ein Punkt von E mit $P \neq P^\gamma$, so ist $P + P^\gamma$ eine Fixgerade von γ.

Es ist ja

$$(P + P^\gamma)^\gamma = P^\gamma + P^{\gamma^2} = P + P^\gamma.$$

2) γ hat mindestens zwei Fixpunkte.

Weil $\gamma \neq 1$ ist, gibt es eine Gerade G mit $G^\gamma \neq G$. Dann ist aber $P := G \cap G^\gamma$ nach der zu 1) dualen Aussage ein Fixpunkt von γ. Wäre P der einzige Fixpunkt von γ, so folgte, dass γ alle Geraden von E, die nicht durch P gehen, fest ließe. Mit I.8.8, angewandt auf $(E^d)_P$, folgte $\gamma = 1$. Dieser Widerspruch zeigt die Gültigkeit von 2).

3) Jeder Punkt von E liegt auf einer Fixgeraden von γ.

Ist P ein Punkt von E, der kein Fixpunkt ist, so ist $P + P^\gamma$ nach 1) eine Fixgerade durch P. Ist P Fixpunkt, so gibt es nach 2) einen weiteren Fixpunkt Q. Dann ist $P + Q$ eine Fixgerade durch P.

a) Wir nehmen nun an, dass γ keinen Rahmen punktweise festlässt. Es seien P, Q und R drei nicht kollineare Fixpunkte von γ und X sei ein Punkt, der auf keiner der Geraden $P+Q$, $Q+R$, $R+P$ liegt. Nach 3) gibt es eine Fixgerade G durch X. Diese ist von den Geraden $P+Q$, $Q+R$, $R+P$ verschieden, da X auf keiner dieser Geraden liegt. Weil die Fixpunktmenge von γ keinen Rahmen enthält, geht G durch einen der Punkte P, Q, R. Wir dürfen annehmen, dass $R \leq G$ ist. Ist H eine Fixgerade von γ, die von $P+Q$, $Q+R$, $R+P$ verschieden ist, so geht H ebenfalls durch einen der Punkte, P, Q und R und aus der Tatsache, dass die Fixpunktmenge von γ keinen Rahmen enthält, sowie aus $R \leq G$ folgt, dass auch $R \leq H$ ist. Es sei schließlich J eine Gerade durch R. Ist $J = P+R$ oder $J = Q+R$, so ist J eine Fixgerade von γ. Ist $J \neq P+Q$, $P+R$, so gibt es einen Punkt $Y \leq J$ mit $Y \neq R$ und $Y \leq P+Q$. Nun ist Y nach 3) in einer Fixgeraden L enthalten. Ferner ist, wie wir bereits wissen, $R \leq L$, woraus $L = J$ folgt. Damit ist gezeigt, dass γ eine Zentralkollineation mit dem Zentrum R ist.

Wir dürfen des Weiteren annehmen, dass alle Fixpunkte von γ kollinear sind. Weil γ nach 2) mindestens zwei Fixpunkte hat, gibt es eine Fixgerade G von γ, die alle Fixpunkte trägt. Die von γ in E_G induzierte Kollineation hat dann keine Fixpunkte in E_G, so dass jeder Punkt von E_G wegen 3) auf genau einer Fixgeraden liegt. Dies besagt wiederum, dass die zu E_G gehörenden Fixgeraden von γ gerade die Geraden einer Parallelschar von E_G sind, so dass γ als Elation erkannt ist.

b) Die Menge der Fixpunkte von γ enthalte einen Rahmen. Dann ist klar, dass die Menge F der Fixpunkte und Fixgeraden von γ eine Unterebene von E bilden. Weil γ auch eine involutorische Kollineation von E^d ist, folgt, dass außer 3) auch die zu 3) duale Aussage gilt, so dass also jeder Punkt von E auf einer Geraden von F und jede Gerade von E durch einen Punkt von F geht. Damit ist alles bewiesen.

Ist E eine projektive Ebene und ist F eine von E verschiedene Unterebene von F, so heißt F *Baerunterebene* von F, wenn jeder Punkt von E auf einer Geraden von F liegt und jede Gerade von E einen Punkt von F trägt. Eine involutorische Kollineation einer projektiven Ebene, die eine Baerunterebene elementweise festlässt, heißt *Baerinvolution*.

Baerunterebenen und Baerinvolutionen kann es bei endlichen projektiven Ebenen nur geben, wenn die Ordnung der Ebene ein Quadrat ist. Dies besagt der folgende Satz.

9.2. Satz. *Es sei E eine endliche projektive Ebene der Ordnung n. Ist F eine von E verschiedene Unterebene von E der Ordnung r und liegt jeder Punkt von E auf einer Geraden von F, so ist $n = r^2$.*

Beweis. F hat r^2+r+1 Punkte und ebenso viele Geraden. Da jeder Punkt von E, der nicht zu F gehört, auf einer und dann auch auf nur einer Geraden von F liegt, ist die Anzahl der Punkte von E gleich

$$r^2 + r + 1 + (r^2 + r + 1)(n + 1 - r - 1).$$

Andererseits ist die Anzahl auch gleich n^2+n+1. Also ist

$$\begin{aligned}0 &= n^2+n+1-r^2-r-1-(r^2+r+1)(n-r)\\ &= (n-r)(n+r+1-r^2-r-1)\\ &= (n-r)(n-r^2).\end{aligned}$$

Weil $F \neq E$ ist, ist $r \neq n$ und daher $n = r^2$, q. e. d.

9.3. Korollar *Es sei E eine endliche projektive Ebene der Ordnung n und Γ sei eine Kollineationsgruppe von E, deren Ordnung eine Potenz von 2 ist. Sind die Fixpunkte von Γ die Punkte einer Unterebene der Ordnung m von E, so gibt es eine ganze Zahl a mit $n = m^{2^a}$.*

Beweis. Die Fixpunkte von Γ seien die Punkte der Unterebene U. Ist $\Gamma = \{1\}$, so ist $U = E$ und daher $n = m$. Es sei also $\Gamma \neq \{1\}$. Es gibt dann eine Involution $\rho \in Z(\Gamma)$. Weil Γ einen Rahmen punktweise festlässt, lässt ρ nach 9.1 und 9.2 eine Unterebene F der Ordnung r mit $r^2 = n$ punktweise fest. Da ρ im Zentrum von Γ liegt, induziert Γ eine Kollineationsgruppe Γ^* auf F. Da alle Fixpunkte von Γ auch Fixpunkte von ρ sind, ist U eine Unterebene von F. Nun ist ρ im Kern des Homomorphismus $*$ von Γ auf Γ^* enthalten, so dass $|\Gamma^*| < |\Gamma|$ ist. Nach Induktionsannahme gibt es folglich eine natürliche Zahl a mit $r = m^{2^{a-1}}$. Daher ist $n = m^{2^a}$, q. e. d.

9.4. Satz. *Es sei E eine projektive Ebene und P, Q und R seien drei nicht kollineare Punkte von E. Ist ρ eine involutorische Perspektivität aus $\Delta(P, Q+R)$ und σ eine involutorische Perspektivität aus $\Delta(Q, R+P)$, so ist $\rho\sigma = \sigma\rho$ und $\rho\sigma$ ist eine involutorische Streckung aus $\Delta(R, P+Q)$.*

Beweis. Es ist $\rho^{-1}\sigma\rho \in \Delta(Q^\rho, (R+P)^\rho) = \Delta(Q, R+P)$ und daher

$$\sigma^{-1}\rho^{-1}\sigma\rho \in \Delta(Q, R+P).$$

Ferner ist $\sigma^{-1}\rho^{-1}\sigma \in \Delta(P^\sigma, (Q+R)^\sigma) = \Delta(P, Q+R)$, woraus

$$\sigma^{-1}\rho^{-1}\sigma\rho \in \Delta(P, Q+R)$$

folgt. Also hat $\sigma^{-1}\rho^{-1}\sigma\rho$ die beiden verschiedenen Zentren P und Q und ist folglich nach II.1.1 gleich 1. Also ist $\rho\sigma = \sigma\rho$. Hieraus folgt weiter $(\rho\sigma)^2 = 1$. Weil $P \neq Q$ ist, ist überdies $\rho\sigma \neq 1$. Folglich hat $\rho\sigma$ auf $Q+R$ nur die Fixpunkte Q und R. Hieraus folgt, dass $\rho\sigma$ keine Baerinvolution ist, da sie sonst mindestens drei Fixpunkte auf $Q+R$ haben müsste. Also ist $\rho\sigma$ nach 9.1 eine Zentralkollineation. Da $Q+R$ eine Fixgerade ist, die von der Achse von $\rho\sigma$ verschieden ist, geht sie durch das Zentrum von $\rho\sigma$. Nun wirkt $\rho\sigma$ auf den Punkten von $R+P$ wie ρ, da σ alle Punkte dieser Geraden festlässt. Also ist auch $R+P$ eine Gerade durch das Zentrum von $\rho\sigma$, so dass R das Zentrum von $\rho\sigma$ ist. Weil schließlich $P+Q$ eine Fixgerade von $\rho\sigma$ ist, die nicht durch R geht, ist $P+Q$ die Achse von $\rho\sigma$. Damit ist alles bewiesen.

Der nächste Satz ist wieder rein technischer Natur.

9.5. Satz. *Es sei E eine endliche projektive Ebene und (P, G) sei ein nicht inzidentes Punkt-Geradenpaar von E. Gibt es für jedes Punktepaar A, B mit $A \neq B$ und A, $B \leq G$ eine involutorische Streckung mit dem Zentrum A und der Achse $B + P$, so hat E Primzahlpotenzordnung.*

Beweis. Die Ordnung von n ist ungerade, da E involutorische Streckungen besitzt. Es sei Π die von allen involutorischen Streckungen, deren Zentren auf G liegen und deren Achsen durch P gehen, erzeugte Kollineationsgruppe von E. Nach 7.1 ist dann $\mathrm{E}(B, B+P) \subseteq \Pi$ und $|\mathrm{E}(B, B+P)| = n$ für alle Punkte B auf G. Somit ist Π zweifach transitiv auf der Menge der Punkte von G. Schließlich ist, falls A und B zwei verschiedene Punkte auf G sind, $\Pi(A, B+P)\mathrm{E}(B, B+P)$ eine Frobeniusgruppe gerader Ordnung und $\mathrm{E}(B, B+P)$ ist ein Normalteiler von Π_B. Aus 8.6 folgt daher die Behauptung.

9.6. Satz. *Es sei E eine endliche projektive Ebene, U sei eine Gerade von E und Δ sei eine Kollineationsgruppe von E_U. Gilt dann*

a) *Ist (P, G) eine Fahne von E_U, so gibt es eine involutorische Streckung $\gamma \in \Delta$ mit $P^\gamma = P$ und $G^\gamma = G$,*

b) *Sind A und B Punkte auf U, sind G und H Geraden von E_U mit $B \leq G, H$ und gibt es eine involutorische Streckung $\gamma \in \Delta$ mit $A^\gamma = A$, $B^\gamma = B$ und $G^\gamma = G$, so gibt es auch eine involutorische Streckung $\delta \in \Delta$ mit $A^\delta = A$, $B^\delta = B$ und $H^\delta = H$,*

so ist die Ordnung von E eine Primzahlpotenz.

Beweis. Wir betrachten zunächst den Fall, dass Δ keine involutorische Streckung enthält, deren Zentrum ein Punkt von E_U ist. Es sei γ eine nach a) existierende involutorische Streckung aus Δ. Ferner sei A das Zentrum und G die Achse von γ. Dann ist $A \leq U$ und $G \neq U$. Setze $B := G \cap U$. Weil γ die Punkte A und B sowie die Gerade G festlässt, gibt es nach b) eine involutorische Streckung $\delta \in \Delta$ mit $A^\delta = A$, $B^\delta = B$ und $H^\delta = H$, wobei H eine beliebig vorgegebene, jedoch von U verschiedene Gerade durch B ist. Wegen $\delta \in \Delta$ ist entweder A oder B das Zentrum von δ. Wäre B das Zentrum von δ so läge A nach II.1.3 auf der Achse J von δ. Nach 9.4 wäre dann $\gamma\delta$ eine involutorische Streckung mit dem Zentrum $G \cap J$ und der Achse $A + B = U$. Somit enthielte Δ doch eine involutorische Streckung mit einem Zentrum in E_U. Dieser Widerspruch zeigt, dass A das Zentrum von δ ist. Dann ist aber H nach II.1.3 die Achse von δ. Aus dem zu Satz 7.1 dualen Satz folgt daher $|\mathrm{E}(A, U)| = n$ Es sei C ein von A verschiedener Punkt auf U. Gibt es in Δ eine involutorische Streckung mit dem Zentrum C, so ist auch $|\mathrm{E}(C, U)| = n$. Wegen $A \neq C$ ist E_U eine Translationsebene, so dass n nach II.1.16 Potenz einer Primzahl ist. Wir dürfen daher annehmen, dass A Zentrum aller involutorischen Streckungen aus Δ ist. Es sei nun G eine Gerade von E, die nicht durch A geht. Nach a) gibt es eine involutorische Streckung $\rho \in \Delta$, die G invariant lässt. Weil A das Zentrum von ρ ist, ist G nach II.1.3 die Achse von ρ. Nach 7.1 ist daher E^d eine Translationsebene bez. A, so dass n auch in diesem Falle Potenz einer Primzahl ist.

Wir betrachten nun den Fall, dass es genau einen Punkt in E_U gibt, der Zentrum einer involutorischen Streckung aus Δ ist. Es sei P dieser Punkt.

Dann ist P ein Fixpunkt von Δ. Es seien A und B zwei verschiedene Punkte auf U und X sei ein von P und B verschiedener Punkt auf $P+B$. Nach a) gibt es eine involutorische Streckung $\rho \in \Delta$ mit $X^\rho = X$ und $(X+A)^\rho = X+A$. Wegen $P^\rho = P$ und $U^\rho = U$ ist dann $(P+X)^\rho = P+X$ sowie

$$B^\rho = \big(U \cap (P+X)\big)^\rho = U^\rho \cap (P+X)^\rho = U \cap (P+X) = B.$$

Somit hat ρ drei verschiedene Fixpunkte auf $P+B$, so dass $P+B$ die Achse von ρ ist. Schließlich ist

$$A^\rho = \big(U \cap (A+X)\big)^\rho = U^\rho \cap (A+X)^\rho = U \cap (A+X) = A$$

und $A \not\leq P+B$, so dass A nach II.1.3 das Zentrum von ρ ist. Anwendung von 9.5 liefert, dass n auch in diesem Falle Potenz einer Primzahl ist.

Es bleibt der Fall zu betrachten, dass wenigstens zwei Punkte in E_U Zentren von involutorischen Streckungen aus Δ sind.

Wir nehmen zunächst weiter an, dass jede Gerade von E_U ein in E_U liegendes Zentrum einer involutorischen Streckung aus Δ trägt. Mit k_G bezeichnen wir die Anzahl dieser Zentren auf der Geraden G. Dann ist $k_G \geq 1$ für alle Geraden G von E_U und $k_G \geq 2$ für wenigstens eine Gerade. Da $n(n+1)$ die Anzahl der Geraden von E_U ist, ist

$$\sum_G k_G > n(n+1).$$

Andererseits gilt nach 1.2 a) die Gleichung

$$v(n+1) = \sum_G k_G,$$

wenn v die Anzahl der Punkte von E_U ist, die Zentren von involutorischen Streckungen aus Δ sind. Also ist $v \geq n+1$. Hieraus folgt mit 7.1 und 7.7, dass n Potenz einer Primzahl ist.

Wir dürfen des Weiteren annehmen, dass es eine Gerade G von E_U gibt, die kein Zentrum einer involutorischen Perspektivität aus Δ trägt. Setze $A := G \cap U$. Es sei B ein von A verschiedener Punkt auf U. Ferner sei P ein Punkt von E_U, der Zentrum einer involutorischen Streckung aus Δ ist. Es gibt dann eine involutorische Streckung in Δ mit den Fixelementen A, B und $A+P$. Nach b) gibt es dann auch eine involutorische Streckung $\rho \in \Delta$ mit den Fixelementen A, B und G. Wäre U die Achse von ρ, so wäre wegen $G^\rho = G \neq U$ das Zentrum von ρ ein von A verschiedener Punkt auf G, im Widerspruch zu der Wahl von G. Also sind A und B die einzigen Fixpunkte von ρ auf U. Da B beliebig gewählt war, folgt mit 7.10, dass $\Delta_{A,G}$ die von A verschiedenen Punkte von U transitiv permutiert.

Enthält Δ eine von 1 verschiedene Elation mit der Achse U und dem Zentrum $B \neq A$, so folgt wiederum $|\mathrm{E}(U)| \geq n+1$, so dass n nach 7.7 Potenz einer Primzahl ist. Wir dürfen daher annehmen, dass alle von Eins verschiedenen Elationen aus Δ, deren Achse U ist, das Zentrum A haben. Nun enthält Δ nach 7.2 eine von 1 verschiedene Elation mit der Achse U. Somit ist $\Delta(A,U) \neq \{1\}$,

so dass A ein Fixpunkt von Δ ist. Es sei P ein von A verschiedener Punkt auf G und B sei ein von A verschiedener Punkt auf U. Nach a) gibt es eine involutorische Streckung $\sigma \in \Delta$ mit $P^\sigma = P$ und $(P + B)^\sigma = P + B$. Dann ist aber $A^\sigma = A$ und $B^\sigma = B$. Weil U nicht die Achse von σ sein kann, P wäre ja sonst Zentrum, sind A und B die einzigen Fixpunkte von σ auf U. Mit Hilfe von 7.10 folgt wiederum, dass $\Delta_{A,P}$ auf der Menge der von A verschiedenen Punkte von U transitiv operiert. Ist B das Zentrum von σ, so ist $G = A + P$ die Achse von σ und aus der Transitivität von $\Delta_{A,P}$ auf der Menge der von A verschiedenen Punkte von U folgt, dass $|\Delta(A,G)| = n$ ist. Ist B nicht das Zentrum von σ, so ist A das Zentrum und $P + B$ die Achse von σ. Die Transitivität von $\Delta_{Q,P}$ auf der Menge der von A verschiedenen Punkte von U impliziert auch in diesem Falle, dass —$\Delta_{A,G}| = n$ ist. Nun ist aber $\Delta(A,U) \neq \{1\}$, wie wir bereits bemerkten, so dass $|\Delta(A)| \geq n+1$ ist. Aus 7.7 folgt somit, dass auch im letzten Falle n Potenz einer Primzahl ist. Damit ist der Satz bewiesen.

9.7. Satz. *Ist E eine endliche projektive Ebene, ist U eine Gerade von E und ist K eine Kollineationsgruppe von E_U, so sind die folgenden Aussagen äquivalent:*

a) *K operiert auf der Menge der Geraden von E_U transitiv.*

b) *K operiert auf der Menge der Punkte von E_U und auch auf der Menge der Punkte von U transitiv.*

c) *K ist transitiv auf der Menge der Fahnen von E_U.*

Beweis. a) impliziert b): Dass die Geradentransitivität von K auf E_U die Transitivität von K auf der Menge der Punkte nach sich zieht, ist unmittelbar einsichtig. Dass K auch auf der Menge der Punkte von E_U transitiv ist, folgt aus 5.5.

b) impliziert c): Es seien (P,G) und (Q,H) zwei Fahnen von E_U. Auf Grund der Transitivität von K auf der Menge der Punkte von E_U dürfen wir annehmen, dass $P = Q$ ist. Es ist dann $G = P + (G \cap U)$ und $H = P + (H \cap U)$. Die Anzahl der Punkte von E_U ist n^2 und die Anzahl der Punkte von U ist $n + 1$. Weil n^2 und $n + 1$ teilerfremd sind, ist K_P nach 8.1 transitiv auf der Menge der Punkte von U. Es gibt also ein $\kappa \in K_P$ mit $(G \cap U)^\kappa = H \cap U$. Es folgt $P^\kappa = P$ und $G^\kappa = H$.

c) impliziert a): Banal.

Eine unmittelbare Folgerung ist

9.8. Korollar *Es sei E eine endliche projektive Ebene der Ordnung n. Ferner sei U eine Gerade von E und K eine Kollineationsgruppe von E_U, die die Geraden von E_U transitiv permutiert. Ist dann (P,G) eine Fahne von E_U und A ein Punkt auf U und setzt man $k := |K_{P,G}|$, so ist $|K| = n^2(n+1)k$, $|K_A| = n^2k$, $|K_G| = nk$, $|K_P| = (n+1)k$ und $|K_{A,P}| = k$.*

Ferner gilt

9.9. Satz. *Es sei E eine endliche projektive Ebene, U sei eine Gerade von E und K sei eine Kollineationsgruppe von E_U. Genau dann ist K auf der Menge*

der Punkte von E_U transitiv, wenn K_A für jeden Punkt A auf U auf der Menge der mit A inzidierenden Geraden von E_U transitiv ist.

Beweis. Es sei s die Anzahl der in U enthaltenen Punktbahnen von K.

Es sei K transitiv auf der Menge der Punkte von E_U. Dann hat K genau $s+1$ Punktbahnen in E und daher nach 3.4 auch genau $s+1$ Geradenbahnen. Weil $\{U\}$ eine dieser Geradenbahnen ist, zerfällt die Menge der Geraden von E_U unter K in genau s Bahnen. Es seien $\Pi_1, \ldots, \Pi_s$ die in U enthaltenen Punktbahnen von K. Wir setzen

$$\Gamma_i := \{G \mid G \text{ ist Gerade von } E_U \text{ mit } G \cap U \in \Pi_i\}$$

für $i := 1, \ldots, s$. Offensichtlich ist jedes Γ_i invariant unter K und somit Vereinigung von Geradenbahnen von K. Weil K in E_U genau s Geradenbahnen hat, folgt, dass die Γ_i allesamt Geradenbahnen von K sind. Es sei schließlich A ein Punkt auf U und G und H seien zwei mit A inzidierende Geraden von E_U. Es gibt ein i mit $A \in \Pi_i$. Es folgt $G, H \in \Gamma_i$. Es gibt daher ein $\kappa \in K$ mit $G^\kappa = H$. Es folgt

$$A^\kappa = (G \cap U)^\kappa = G^\kappa \cap U^\kappa = H \cap U = A,$$

so dass sogar $\kappa \in K_A$ gilt.

Wir nehmen umgekehrt an, dass K_A für alle $A \leq U$ die Menge der Geraden von E_U, die durch A gehen, transitiv permutiert. K zerlegt dann offensichtlich die Menge der Geraden von E_U in s Bahnen, so dass K genau $s+1$ Geradenbahnen in E hat. Folglich hat K auch genau $s+1$ Punktbahnen in E. Da s von diesen Punktbahnen in U enthalten sind, besteht die restliche Bahn aus den Punkten von E_U. Damit ist der Satz bewiesen.

9.10. Korollar. *Es sei E endliche projektive Ebene, U sei eine Gerade von E und K sei eine Kollineationsgruppe von E_U, die auf der Menge der Geraden von E_U transitiv ist. Sind A und B Punkte von U und sind G und H durch B gehende Geraden von E_U, so ist $|K_{A,B,G}| = |K_{A,B,H}|$.*

Beweis. Wegen $\mathrm{ggT}(n^2, n+1) = 1$ folgt aus 9.7 und 8.1, dass K_A auf der Punktmenge von E_U transitiv operiert. Aus 9.9 folgt daher die Transitivität von $K_{A,B}$ auf der Menge der durch B gehenden Geraden von E_U. Hieraus folgt die Behauptung.

Die nächsten drei Sätze sind die Höhepunkte dieses Abschnitts. 9.12 wurde von Ostrom & Wagner vor dem von Wagner stammenden nächsten Satz bewiesen, aus dem er wiederum sehr einfach folgt.

9.11. Satz. *Es sei E eine endliche projektive Ebene und U sei eine Gerade von E. Ist K eine Kollineationsgruppe von E_U, die die Geraden von E_U transitiv permutiert, so ist E eine Translationsebene bez. U und* $\mathrm{E}(U)$ *ist in K enthalten.*

Beweis. Es sei n die Ordnung von E. Ist (P, G) eine Fahne von E_U, so setzen wir $k := |K_{P,G}|$.

1. Fall: n ist gerade. Es sei 2^a die höchste in n aufgehende Potenz von 2. Dann ist $a \geq 1$. Es sei Σ eine 2-Sylowgruppe von K. Nach 9.8 ist $|\Sigma| = 2^{2a+b}$.

Schließlich sei σ eine Involution aus dem Zentrum $Z(\Sigma)$ von Σ. Ist σ eine Perspektivität, so ist σ, da n gerade ist, eine Elation. Nach 9.1 ist σ daher entweder eine Elation oder aber die Fixpunkte von σ sind die Punkte einer Baerunterebene F von E. Hat F die Ordnung r, so ist $r^2 = n$ nach 9.3. Sind die Fixpunkte von σ die Punkte einer Baerunterebene, so hat σ genau $r^2 + r + 1 = n + r + 1$ Fixpunkte. Wegen $U^\sigma = U$ ist U eine Gerade von F, so dass auf U genau $r + 1$ Fixpunkte von σ liegen, dh., genau n der Fixpunkte von σ liegen in E_U. Ist σ eine Elation und ist U nicht die Achse von σ, so hat σ genau $n + 1$ Fixpunkte, von denen wiederum genau n in E_U liegen. Es gilt also, dass genau n der Fixpunkte von σ in E_U liegen, wenn wenigstens einer der Punkte von E_U ein Fixpunkt von σ ist.

Es sei S die Menge der in E_U liegenden Fixpunkte von σ. Dann ist $S = \emptyset$ oder $|S| = n$, wie wir gerade gesehen haben. Wir nehmen an, dass $|S| = n$ ist. Wegen $\sigma \in Z(\Sigma)$ ist S unter Σ invariant. Folglich ist S Vereinigung von Bahnen von Σ. Nach 8.2 ist die Länge jeder Bahn von Σ durch 2^{2a} teilbar, da K ja auf der Menge der n^2 Punkte von E_U transitiv operiert. Also ist 2^{2a} Teiler von $|S| = n$. Hieraus folgt $2a \leq a$, was wegen $a \geq 1$ ein Widerspruch ist. Also ist $S = \emptyset$, was wiederum besagt, dass σ eine Elation mit der Achse U ist. Weil K auf der Menge der Punkte von U transitiv operiert, sind die Gruppen $K(P, U)$ mit $P \leq U$ in K konjugiert und haben daher alle die Ordnung $h \geq 2$. Nach 7.9 ist folglich $h = n$ und $K(P, U) = \mathrm{E}(P, U)$ für alle $P \leq U$. Damit ist der Satz im Falle, dass n gerade ist, bewiesen.

2. Fall: n ist ungerade. Wir zeigen zunächst, dass dann n Potenz einer Primzahl ist.

Es sei F eine Unterebene von E mit den beiden Eigenschaften:

j) Es gibt eine 2-Untergruppe von K, so dass die Fixpunkte dieser Untergruppe gerade die Punkte von F sind.

ij) Es gibt keine echte Unterebene von F, so dass die Punkte dieser Unterebene gerade die Fixpunkte einer 2-Untergruppe von K sind.

Weil die Gruppe, die nur aus der 1 besteht, eine 2-Untergruppe von K ist, hat E die Eigenschaft j). Weil E endlich ist, folgt daher, dass E auch eine Unterebene F besitzt, die die beiden Eigenschaften j) und ij) hat.

Es sei Σ eine 2-Untergruppe von K, die maximal ist bezüglich der Eigenschaft, dass die Fixpunkte von Σ gerade die Punkte von F sind. Ferner sei 2^a die höchste in $n+1$ und 2^b die höchste in k aufgehende Potenz von 2. Schließlich sei $|\Sigma| = 2^c$. Weil n ungerade ist, ist $n + 1$ gerade und daher $a \geq 1$.

a) Ist (P, G) eine Fahne von F_U, so gibt es eine involutorische Streckung γ von F_U mit $P^\gamma = P$ und $G^\gamma = G$, die von einer Kollineation aus K induziert wird.

Σ ist eine Untergruppe von $K_{P,G}$. Wegen $|K_{P,G}| = k$ ist die Ordnung 2^c von Σ ein Teiler von 2^b. Nun ist 2^{a+b} die Ordnung einer 2-Sylowgruppe von K und es ist $a \leq 1$. Daher ist Σ keine 2-Sylowgruppe von K. Es gibt folglich eine 2-Untergruppe Σ^* von K, die Σ enthält und für die $|\Sigma^* : \Sigma| = 2$ ist. Hieraus folgt, dass Σ ein Normalteiler von Σ^* ist, was wiederum impliziert, dass F von Σ^* invariant gelassen wird. Aus der Maximalität von Σ folgt, dass Σ^* eine

Kollineationsgruppe der Ordnung 2 in F induziert. Aus der Minimalität von F folgt weiter, dass das erzeugende Element σ dieser Gruppe eine Perspektivität ist. Ist m die Ordnung von F, so ist n nach 9.3 eine Potenz von m, so dass mit n auch m ungerade ist. Daher ist σ eine Streckung von F_U. Hieraus folgt wiederum die Existenz einer Fahne (Q, J) von F_U mit $Q^\sigma = Q$ und $J^\sigma = J$. Also ist $\Sigma^* \subseteq K_{Q,J}$, so dass wegen $|K_{Q,J}| = k$ die Ungleichung $2^c < 2^b$ gilt. Dies impliziert, dass Σ keine 2-Sylowgruppe von $K_{P,G}$ ist. Es gibt daher bereits in $K_{P,G}$ eine Gruppe Σ^* mit $|\Sigma^* : \Sigma| = 2$. Dann gibt es aber, wie wir gesehen haben, eine involutorische Streckung von F_U, die die Fahne (P, G) invariant lässt und die von einer Kollineation aus K induziert wird.

b) A und B seien zwei auf U liegende Punkte von F und G und H seien zwei Geraden von F_U mit $B \leq G$, H. Gibt es dann eine involutorische Streckung von F_U mit den Fixelementen A, B und G, die von einer Kollineation aus K induziert wird, so gibt es eine ebensolche Streckung mit den Fixelementen A, B und H.

Es sei Λ der Stabilisator von F in K und $\bar{\Lambda}$ sei die Untergruppe von Λ, die F elementweise festlässt. Dann ist $\Sigma \subseteq \bar{\Lambda}$ und $\bar{\Lambda}$ ist ein Normalteiler von $\Lambda_{A,B,G}$. Aufgrund unserer Annahme enthält $\Lambda_{A,B,G}/\bar{\Lambda}$ ein Element der Ordnung 2. Wegen $\Lambda_{A,B,G} \subseteq K_{A,B,G}$ ist somit Σ keine 2-Sylowgruppe von $K_{A,B,G}$. Nach 9.10 ist $|K_{A,B,G}| = |K_{A,B,H}|$, so dass Σ auch keine 2-Sylowgruppe von $K_{A,B,H}$ ist. Es gibt folglich eine 2-Untergruppe Σ^* von $K_{A,B,H}$ mit $|\Sigma^* : \Sigma| = 2$. Wie der Beweis von a) zeigt, induziert Σ^* eine Kollineationsgruppe der Ordnung 2 in F_U, deren erzeugendes Element eine involutorische Streckung mit den Fixelementen A, B und H ist. Damit ist auch b) bewiesen. Die Gültigkeit von a) und b) impliziert nun nach 9.6, dass m Potenz einer Primzahl ist. Weil schließlich n, wie wir bereits bemerkten, Potenz von m ist, ist auch n Potenz einer Primzahl.

Wir sind nun in der Lage den Beweis von 9.11 zu beenden. Wie wir gesehen haben, ist $n = p^r$ mit einer Primzahl p. Es sei p^s die höchste in k aufgehende Potenz von p. Ist dann Π eine p-Sylowgruppe von K, so ist $|\Pi| = p^{2r+s}$. Weil K auf der Menge der p^{2r} Punkte von E_U transitiv ist, ist auch Π nach 8.2 auf der Menge der Punkte von E_U transitiv. Andererseits hat Π auf U einen Fixpunkt A, da die Anzahl $n + 1$ der Punkte auf U nicht durch p teilbar ist. Wegen $|\Pi| = p^{2r+s} > p^r$ gibt es einen von A verschiedenen Punkt B auf U mit $\Pi_B \neq \{1\}$. Der Punkt B sei so gewählt, dass $|\Pi_B| \geq |\Pi_Q|$ ist für alle von A verschiedenen Punkte Q auf U. Es sei C ein von A verschiedener Fixpunkt von Π_B. Wegen $\Pi_B = \Pi_{B,C} \subseteq \Pi_C$ und $|\Pi_B| \geq |\Pi_C|$ ist dann $\Pi_B = \Pi_C$. Weil Π auf der Menge der Punkte von E_U transitiv ist, ist Π_B auf der Menge der durch C gehenden Geraden von E_U nach 9.9 transitiv. Es sei $\bar{\Pi}$ eine p-Sylowgruppe von K_B, die Π_B enthält. Dann ist $\Pi_B \subseteq \bar{\Pi}_A$. Weil $|K_B| = n^2 k$ ist, ist $\bar{\Pi}$ sogar eine p-Sylowgruppe von K. Daher sind Π und $\bar{\Pi}$ konjugiert. Aus der Maximalität von Π_B folgt daher $\Pi_B = \bar{\Pi}_A$, so dass Π_B auch auf der Menge der durch A gehenden Geraden von E_U transitiv ist.

Es sei $1 \neq \tau \in Z(\Pi_B)$. Weil τ zwei Fixpunkte hat, nämlich A und B, hat τ nach 3.2 auch zwei Fixgeraden. Es gibt daher eine Gerade G von E_U mit $G^\tau = G$. Gibt es ein Element $\mu \in \Pi_B$ mit $(G \cap U)^\pi \neq G \cap U$, so ist $G \cap G^\mu$ ein

Punkt von E_U. Wegen $\tau \in Z(\Pi_B)$ ist

$$(G \cap G^\mu)^\tau = G^\tau \cap G^{\mu\tau} = G \cap G^{\tau\mu} = G \cap G^\mu.$$

Daher ist $A + (G \cap G^\mu)$ eine Fixgerade von τ, die U in einem Fixpunkt von Π_B, nämlich A, schneidet. Wir dürfen daher annehmen, dass $C := G \cap U$ ein Fixpunkt von Π_B ist. Aus der Transitivität von Π_B auf der Menge der durch C gehenden Geraden von E_U, folgt, dass τ alle Geraden durch C einzeln invariant lässt, so dass τ zentral mit dem Zentrum C ist. Ist λ die Anzahl der Fixpunkte von Π_B auf U, so ist $\lambda \equiv 1 \bmod p$ und $\lambda \geq 2$. Daher ist sogar $\lambda \geq 3$. Somit hat τ auf U mindestens drei Fixpunkte, so dass U die Achse von τ ist. Also ist $K(C, U) \neq \{1\}$. Hieraus folgt wiederum genauso wie im Falle eines geraden n, dass E eine Translationsebene bez. U ist und dass $\mathrm{E}(U)$ in K enthalten ist. Damit ist der Satz bewiesen.

Wir benutzen nun den gerade bewiesenen Satz, um den folgenden von Ostrom & Wagner stammenden Satz zu bewiesen, der, wie schon gesagt, der ältere der beiden Sätze ist.

9.12. Satz. *Ist E eine endliche projektive Ebene und ist K eine Kollineationsgruppe von E, die auf der Menge der Punkte von E zweifach transitiv operiert, so ist E desarguessch und K enthält die kleine projektive Gruppe von E.*

Beweis. Nach 3.5 ist K auch auf der Menge der Geraden von E zweifach transitiv. Ist U eine Gerade von E, so ist also K_U auf der Menge der Geraden von E_U noch transitiv. Nach 9.11 ist E_U folglich eine Translationsebene und $E(U)$ ist in K_U enthalten. Somit ist E eine Moufangebene und K enthält die kleine projektive Gruppe von E. Weil E endlich ist, ist E nach 6.1 desarguessch.

9.13. Satz. *Es sei E eine endliche projektive Ebene und K sei eine Kollineationsgruppe von E. Ist K auf der Menge der nicht inzidenten Punkt-Geradenpaare von E transitiv, so ist E desarguessch und K enthält die kleine projektive Gruppe von E.*

Beweis. Es sei (P, G) eine Fahne von E. Dann ist K_G auf der Menge der Punkte von E_G transitiv, so dass $K_{P,G}$ nach 9.9 auf der Menge der von G verschiedenen Geraden durch P transitiv ist. Weil durch P mindestens drei Geraden gehen und G eine beliebige Gerade durch P ist, folgt, dass K_P auf der Menge aller Geraden durch P transitiv operiert. Weil K_P nach Voraussetzung auch auf der Menge der nicht durch P gehenden Geraden transitiv operiert, hat G_P genau zwei Geradenbahnen. Nach 3.4 hat G_P dann auch genau zwei Punktbahnen. Eine davon ist $\{P\}$. Dies besagt, dass K auf der Menge der Punkte von E zweifach transitiv operiert. 9.13 ist daher eine Folge von 9.12.

10. Endliche projektive Räume

Es sei T ein 2-(v, k, λ)-Blockplan. Sind P und Q zwei verschiedene Punkte von T und sind $c_1, \ldots, c_\lambda$ die mit P und Q inzidierenden Blöcke, so definieren wir die *Gerade* $P + Q$ durch

$$P + Q := \{X \mid X \mathrm{\ I\ } c_1, \ \ldots, \ c_\lambda\}.$$

Da durch zwei verschiedene Punkte von T stets genau λ Blöcke gehen, ist jede Gerade durch irgend zwei auf ihr liegende Punkte eindeutig bestimmt.

Sind P, Q und R drei nicht kollineare Punkte von T, so definieren wir die durch P, Q und R bestimmte *Ebene* $P+Q+R$ durch

$$P+Q+R := \{X \mid X \mathrel{\mathrm{I}} c_1,\ \ldots,\ c_i\},$$

wobei $c_1, \ldots, c_i$ die mit P, Q und R inzidierenden Blöcke sind. Ist $i=0$, so ist $P+Q+R$ die Menge aller Punkte von T. Sind P', Q' und R' drei nicht kollineare Punkte in $P+Q+R$, so ist $P'+Q'+R' \subseteq P+Q+R$ und es kann vorkommen, dass $P'+Q'+R'$ echt in $P+Q+R$ enthalten ist.

10.1. Satz. *Ist T ein 2-Blockplan mit den Parametern v, b, k, r und λ, so sind die folgenden Bedingungen äquivalent:*

a) *Es gibt einen endlichen projektiven Verband L mit $\mathrm{Rg}(L) \geq 3$, so dass T und $L_{1,\mathrm{Rg}(L)-1}$ isomorph sind.*

b) *Es ist $v \geq k+2$ und jede Gerade von T hat mit jedem Block von T einen Punkt gemeinsam.*

c) *Es ist $v \geq k+2$ und auf jeder Geraden von T liegen genau $\frac{b-\lambda}{r-\lambda}$ Punkte.*

Beweis. In jeder projektiven Geometrie, deren Rang mindestens 3 ist, trifft jede Gerade jede Hyperebene und außerhalb jeder Hyperebene liegt mehr als ein Punkt. Daher ist b) eine Folge von a).

Um die Äquivalenz von b) und c) zu beweisen, sei g eine Gerade von T. Durch jeden Punkt P von g gehen r Blöcke, von denen λ die Gerade g enthalten. Die restlichen $r-\lambda$ Blöcke treffen g nur in P. Die Zahl der g treffenden Blöcke ist daher

$$|g|(r-\lambda)+\lambda.$$

Also trifft g genau dann jeden Block, wenn

$$|g|(r-\lambda)+\lambda = b$$

ist, dh. genau dann, wenn

$$|g| = \frac{b-\lambda}{r-\lambda}$$

ist. Dies zeigt die Gleichwertigkeit von b) und c).

Wir setzen jetzt die Gültigkeit von b) und c) voraus. Als erstes zeigen wir, dass die aus den Punkten und Geraden von T bestehende Inzidenzstruktur eine irreduzible projektive Geometrie ist. Durch zwei verschiedene Punkte von T geht natürlich genau eine Gerade. Auf jeder Geraden liegen mindestens drei Punkte. Andernfalls wäre nämlich $\frac{b-\lambda}{r-\lambda} = 2$, so dass jede Gerade genau zwei Punkte trüge. Dann gäbe es aber wegen $v \geq k+2$ eine Gerade, die einen gegebenen Block nicht trifft.

Es seien P, Q und R drei nicht kollineare Punkte und ρ sei die Anzahl der Blöcke, die P, Q und R enthalten. Dann ist $r-\rho$ die Anzahl der Blöcke durch P, die $P+Q+R$ nicht enthalten. Wegen b) trifft jeder dieser Blöcke die Gerade $Q+R$ in genau einem Punkt. Somit ist

$$r-\rho = |Q+R|(\lambda-\rho),$$

so dass ρ wegen $|Q+R| = \frac{b-\lambda}{r-\lambda}$ von der Auswahl von P, Q und R unabhängig ist. Daher ist jede Ebene durch irgend drei in ihr liegende, nicht kollineare Punkte eindeutig bestimmt.

Um zu zeigen, dass auch das Veblen-Young-Axiom gilt, genügt es zu zeigen, dass zwei Geraden, die in einer Ebene liegen, einen Schnittpunkt haben. Es seien also g und h zwei Geraden, die in einer Ebene E und T liegen. Wegen $\rho < \lambda$ gibt es einen Block c mit $h \subseteq c$ und $E \not\subseteq c$. Weil eine Ebene durch irgend drei ihrer Punkte eindeutig bestimmt ist, folgt dass $E \cap c = h$ ist. Wegen b) gibt es einen Punkt $P \in g$ mit $P \mathrel{\mathrm{I}} c$. Wegen $g \subseteq E$ ist daher $P \in E \cap c = h$. Somit haben g und h den Punkt P gemeinsam. Damit ist gezeigt, dass die Inzidenzstruktur aus den Punkten und Geraden von T eine projektive Geometrie ist.

Die Blöcke von T sind offensichtlich Unterräume der eben konstruierten projektiven Geometrie L und da die Hyperebenen von σ die einzigen Unterräume von L sind, die von allen Geraden getroffen werden, folgt, dass die Blöcke von T Hyperebenen von L sind. Nun besagt die fisher'sche Ungleichung, dass $v \leq b$ ist, weil andererseits nach I.7.7 die Anzahl der Hyperebenen von L gleich der Anzahl der Punkte von L ist, ist $b \leq v$. Also ist $b = v$, so dass T in der Tat zu $L_{1,r-1}$ isomorph ist, wenn r der Rang von L ist. Schließlich folgt aus $v \geq k+2$, dass $r \geq 3$ ist. Damit ist der Satz bewiesen.

Wenn man in 10.1 nur $v \geq k+1$ voraussetzt, so erhält man als weitere Beispiele nur noch die Blockpläne $(M, P_{|M|-1}(M), \in)$ mit einer endlichen Menge M, wie der Beweis von 10.1 klar zeigt. Dabei ist $P_{|M|-1}(M)$ die Menge der $(|M|-1)$-Teilmengen von M.

10.2. Satz. *Ist T ein projektiver Blockplan mit $v \geq k+2$, so sind die folgenden Bedingungen äquivalent:*

a) *Es gibt einen Vektorraum V des Ranges $r \geq 3$, so dass T und $L(V)_{1,r-1}$ isomorph sind.*

b) *T besitzt eine auf der Menge der geordneten Tripel nicht kollinearer Punkte transitive Kollineationsgruppe.*

c) *T besitzt eine auf der Menge der nicht inzidenten Punkt-Geradenpaare transitive Kollineationsgruppe.*

Beweis. Es gelte a). Da die Geraden von $L(V)$ gleich dem Schnitt der sie umfassenden Hyperebenen sind, bedeutet Kollinearität in T dasselbe wie Kollinearität in $L(V)_{1,r-1}$. Daher folgt aus der Transitivität der Kollineationsgruppe von $L(V)$ auf der Menge der Rahmen von $L(V)$ die Transitivität dieser Gruppe auf der Menge der geordneten Tripel nicht kollinearer Punkte. Aus a) folgt also b).

c) folgt trivialerweise aus b).

Um zu zeigen, dass a) von c) impliziert wird, zeigen wir zunächst, dass jede Gerade von T jeden Block von T trifft. Es sei G eine Gerade von T und Γ sei der Stabilisator von G in der Kollineationsgruppe von T. Dann ist Γ auf der Menge der nicht mit G inzidierenden Punkte transitiv. Zerlegt Γ die Menge der Punkte auf G in s Bahnen, so hat Γ insgesamt $s+1$ Punktbahnen und daher nach 3.4 auch genau $s+1$ Blockbahnen. Sind c und d Blöcke, die G treffen, jedoch nicht enthalten, so gibt es genau zwei Punkte P und Q auf G mit $P \mathrel{\mathrm{I}} c$

und Q I d. Liegen P und Q in verschiedenen Punktbahnen, so liegen c und d in verschiedenen Blockbahnen von Γ. Somit zerfällt die Menge der Blöcke, die G treffen, aber nicht enthalten, in mindestens s Bahnen unter Γ. Da die Menge der Blöcke, die G enthalten, ebenfalls unter Γ invariant ist, zerfällt die Menge der Blöcke, die G treffen, in mindestens $s+1$ Bahnen unter Γ. Da Γ aber genau $s+1$ Blockbahnen hat, trifft die Gerade G jeden Block von T. Nach 10.1 gibt es daher einen endlichen projektiven Verband L mit $\mathrm{Rg}(L) = r \geq 3$, so dass T und $L_{1,r-1}$ isomorph sind. Ist $r = 3$, so ist T eine projektive Ebene, die nach 9.13 desarguessch ist. Also ist L in jedem Fall eine desarguessche projektive Geometrie. Nach II.6.1 gibt es somit einen Vektorraum, so dass L und $L(V)$ isomorph sind. Damit ist alles bewiesen.

11. Ein Satz von N. Ito

Eine Kollineation eines Blockplanes T heißt *Zentralkollineation* von T mit *Zentrum* P, wenn sie jeden Block durch P invariant lässt.

11.1. Satz. *Es sei T ein Blockplan mit der Eigenschaft, dass zwei verschiedene Blöcke von T höchstens $k-2$ Punkte gemeinsam haben. Ist dann σ eine Zentralkollineation von T und hat σ zwei verschiedene Zentren, so ist $\sigma = 1$.*

Beweis. σ habe die beiden Zentren P und Q. Ist G eine Gerade durch P oder Q, so ist $G^\sigma = G$, da σ ja alle Blöcke durch P bzw. Q festlässt. Ist R ein Punkt mit $R \not\leq P + Q$, so ist $R = (P+R) \cap (Q+R)$, woraus $R^\sigma = R$ folgt. Ist $R \leq P + Q$, so gibt es einen Block c mit $R = (P+Q) \cap c$. Nun enthält c mindestens $k-1$ Fixpunkte, so dass c und c^σ mindestens $k-1$ Punkte gemeinsam haben. Auf Grund unserer Annahme ist daher $c^\sigma = c$. Also ist

$$R^\sigma = \big((P+Q) \cap c\big)^\sigma = (P+Q)^\sigma \cap c^\sigma = (P+Q) \cap c = R.$$

Damit ist gezeigt, dass σ alle Punkte von T festlässt, woraus $\sigma = 1$ folgt.

11.2. Satz. *Es sei G eine auf Ω zweifach transitiv operierende, endliche Permutationsgruppe. Ist U eine Untergruppe von G mit $|G:U| < |\Omega|$, so ist U transitiv auf Ω.*

Beweis. U sei intransitiv. Weil $U \neq \{1\}$ ist, gibt es dann eine Bahn c von U mit $2 \leq |c| < |\Omega|$. Es sei B die Menge aller Bilder von c unter G. Wegen der zweifachen Transitivität von G auf Ω ist dann $T := (\Omega, B, \in)$ ein 2-Blockplan mit $k = |c| < |\Omega| = v$. Nach 2.4 ist daher $v \leq |B|$. Nun ist $|B| = |G:H|$, wobei H der Stabilisator von c in G ist. Weil c eine Bahn von U ist, ist $U \subseteq H$. Somit ist $|G:H| \leq |G:U|$ und daher

$$v \leq |G:H| \leq |G:U| < v,$$

q. e. a.

Nun haben wir alles beisammen, um den folgenden Satz von Ito zu beweisen.

11.3. Satz. *Es sei Π eine Menge von v Punkten und G sei eine auf Π zweifach transitive Permutationsgruppe. Ferner sei c eine Teilmenge von Π mit $2 \leq$*

$|c| < v$ *und es sei* $B := \{c^\gamma \mid \gamma \in G\}$. *Ist dann* c *Bahn einer Untergruppe* Δ *vom Index* v *in* G *und operiert* Δ *auf* c *nicht treu, so besteht* $T := (\Pi, B, \in)$ *aus den Punkten und Hyperebenen einer desarguesschen projektiven Geometrie* $L(V)$ *mit* $\mathrm{Rg}(L(V)) \geq 3$ *und es ist* $\mathrm{PSL}(V) \subseteq G \subseteq \mathrm{P\Gamma L}(V)$.

Beweis. Weil G auf Π zweifach transitiv operiert, ist T ein Blockplan. Ist $\bar{\Delta}$ der Stabilisator von c in G, so ist $\Delta \subseteq \bar{\Delta}$ und somit

$$|B| = |G : \bar{\Delta}| \leq |G : \Delta| = v.$$

Hieraus folgt mittels der fisherschen Ungleichung, dass $|B| = v$ ist. Folglich ist $\bar{\Delta} = \Delta$ und der Blockplan T ist projektiv.

Es sei N die Untergruppe von Δ, die c punktweise festlässt. Da Δ auf c nicht treu operiert, ist $N \neq \{1\}$. Hieraus folgt, dass $|\Pi - c| \geq 2$ ist. Setzt man $k := |c|$, so ist also $v \geq k + 2$. Es sei λ die Anzahl der mit zwei verschiedenen Punkten inzidierenden Blöcke. Sind dann d und c zwei verschiedene Blöcke von T, so ist nach 2.6 auch $|d \cap e| = \lambda$. Nun ist $k(k-1) = \lambda(v-1)$, so dass wegen $k < v - 1$ auch $\lambda < k - 1$ gilt. Wir können daher im Folgenden 11.1 anwenden.

G ist eine Gruppe von Kollineationen von T, die auf Π zweifach transitiv operiert. Nach 3.5 operiert G folglich auch zweifach transitiv auf B.

Wir zeigen nun, dass N auf $\Pi - c$ transitiv ist. Dazu nehmen wir an, dass dies nicht der Fall sei. Wir zeigen dann

a) N operiert regulär auf $\Pi - c$.

Es ist $\Delta = G_c$, so dass Δ wegen der zweifachen Transitivität von G auf B zwei Blockbahnen hat. Nach 3.4 hat Δ auch genau zwei Punktbahnen. Folglich ist Δ auf $\Pi - c$ transitiv. Weil N in Δ normal ist, haben alle in $\Pi - c$ enthaltenen Bahnen von N die gleiche Länge. Die all diesen Bahnen gemeinsame Länge sei t. Es sei $1 \neq \nu \in N$. Ferner sei $P \in \Pi - c$ und es gelte $P^\nu = P$. Ist d ein Block durch P, so ist $|c \cap d| = \lambda$. Daher enthält d mindestens $\lambda + 1$ Fixpunkte von ν. Weil zwei verschiedene Blöcke nur λ Punkte gemeinsam haben, folgt $d^\nu = d$. Somit ist P Zentrum von ν. Weil $\nu \neq 1$ ist, folgt nach 11.1 weiter, dass P der einzige Fixpunkt von ν in $\Pi - c$ ist. Es sei Φ die Bahn von N, die P enthält. Dann ist $|\Phi| = t$ und $\Phi^\nu = \Phi$. Weil ν^i für alle natürliche Zahlen i zentral mit dem Zentrum P ist, folgt mit 11.1, dass die Ordnung von ν Teiler von $t - 1$ ist. Es gibt eine von Φ verschiedene, in $\Pi - c$ enthaltene Bahn Ψ von N. Wegen $|\Psi| = t$ und $\mathrm{ggT}(t, t-1) = 1$ folgt, dass ν einen Fixpunkt in Ψ hat. Wegen $\Phi \cap \Psi = \emptyset$ ist $P \neq Q$, so dass doch $\nu = 1$ ist. Dieser Widerspruch zeigt die Gültigkeit von a).

Setze $t := |N|$. Nach a) ist dann $(v - k)t^{-1}$ die Anzahl der Bahnen von N in $\Pi - c$. Daher ist $k + (b - k)t^{-1}$ die Anzahl der Punktbahnen von N.

Die Gruppe Δ ist auf der Menge der von c verschiedenen Blöcke transitiv. Weil N in Δ normal ist, zerlegt N daher diese Menge in lauter Bahnen gleicher Länge. Ist d ein von c verschiedener Block und ist $u := |N : N_d|$, so ist u die Länge einer solchen Bahn. Daher ist $(v-1)u^{-1}$ die Anzahl der von $\{c\}$ verschiedenen Blockbahnen von N. Insgesamt ist also $1 + (v-1)u^{-1}$ die Anzahl der Blockbahnen von N. Wegen 3.4 gilt somit

b) Es ist $k + (v - k)t^{-1} = 1 + (v - 1)u^{-1}$.

Unser nächstes Ziel ist zu zeigen, dass N eine p-Gruppe ist. Dazu sei p ein Primteiler von $|N|$ und p^a sei die Ordnung einer p-Sylowgruppe Σ von N. Schließlich sei $N_\Delta(\Sigma)$ der Normalisator von Σ in Δ. Weil N ein Normalteiler von Δ ist, liegen alle Konjugierten von Σ in N. Daher gilt

$$\big|\Delta : N_\Delta(\Sigma)\big| = \big|N : N_\Delta(\Sigma) \cap N\big|.$$

Hieraus folgt,

$$|N_\Delta(\Sigma)N| = \frac{|N_\Delta(\Sigma)||N|}{|N_\Delta(\Sigma) \cap N|} = \frac{|N_\Delta(\Sigma)||\Delta|}{|N_\Delta(\Sigma)|} = |\Delta|$$

und damit $\Delta = N_\Delta(\Sigma)N$. (Dies ist das sogenannte Frattiniargument.) Hieraus folgt, dass $N_\Delta(\Sigma)$ auf der Menge der von $\{c\}$ verschiedenen Blockbahnen von N transitiv operiert, da Δ, wie wir schon bemerkten, auf der Menge der von c verschiedenen Blöcke transitiv ist. Es sei x die Anzahl der in einer von $\{c\}$ verschiedenen Blockbahn von N enthaltenen Bahnen von Σ, so folgt daher, dass $(v-1)xu^{-1}$ die Anzahl der von $\{c\}$ verschiedenen Blockbahnen von Σ ist. Also hat Π genau $1 + (v - 1)xu^{-1}$ Blockbahnen. Weil Σ auf $\Pi - c$ regulär operiert, ist $k + (v - k)p^{-a}$ die Anzahl der Punktbahnen von Π. Nach 3.4 gilt daher

c) $k + (v - k)p^{-a} = 1 + (v - 1)xu^{-1}$.

Es sei $t = p^a t'$, $u = p^b u'$ mit $\mathrm{ggT}(p, u') = 1$, sowie $|N_d| = |N|u^{-1} = y = p^c y'$ mit $\mathrm{ggT}(p, y') = 1$. Dann ist $t = |N| = uy$ und daher

d) $a = b + c$ und $t' = u'y'$.

Aus a), b) und c) folgt nun

$$k + t'(v - k)t^{-1} = 1 + \big(k + (v - k)t^{-1} - 1\big)x.$$

Daher ist

e) $(v - k)(t' - x)t^{-1} = (k - 1)(x - 1)$.

Ist P ein Punkt von c, so gibt es $k - 1$ von c verschiedene Blöcke durch P. Da die Menge dieser Blöcke unter N invariant bleibt, ist

f) $k - 1 = du$,

wobei d eine natürliche Zahl ist. Aus b) und f) folgt

$$(v - k)t^{-1} - (v - k)u^{-1} = -(k - 1) + (k - 1) + (k - 1)u^{-1} = -du + d.$$

Mit Hilfe von d) erhalten wir daher

g) $(v - k)(y - 1)t^{-1} = d(u - 1)$.

Multipliziert man die Gleichung g) mit $t' - x$, so erhält man mit Hilfe von e) und f)

$$\begin{aligned} d(u - 1)(t' - x) &= (v - k)(t' - x)t^{-1}(y - 1) \\ &= (k - 1)(x - 1)(y - 1) \\ &= du(x - 1)(y - 1). \end{aligned}$$

Also ist

h) $(u-1)(t'-x) = u(x-1)(y-1)$,

so dass $t' - x \equiv 0 \bmod u'$ ist. Wegen d) gilt daher

i) $x \equiv 0 \bmod u'$.

Es sei Γ eine von $\{c\}$ verschiedene Blockbahn von N und $\Gamma_1, \dots, \Gamma_x$ seien die in Γ enthaltenen Blockbahnen von Σ. Ferner sei c_i ein Block aus Γ_i und N_i bzw. Σ_i sei der Stabilisator von c_i in N bzw. Σ. Wie wir wissen, ist $|N : N_i| = u = p^b u'$. Weil Σ_i in einer p-Sylowgruppe von N_i liegt, folgt, dass p_b ein Teiler von $|\Sigma : \Sigma_i|$ ist, dh., es ist $|\Sigma : \Sigma_i| = p^b u_i$ mit einer natürlichen Zahl u_i. Schließlich gilt wegen

$$|\Gamma_i| = |\Sigma : \Gamma_i| = p^b u_i$$

die Gleichung

$$\sum_{i:=1}^{x} p^b u_i = |\Gamma| = u.$$

Also ist $\sum_{i:=1}^{x} u_i = u'$, woraus wegen $u_i \geq 1$ folgt, dass $x \leq u'$ ist. Zusammen mit i) ergibt das $u' = x$. Hieraus, aus h) und d) folgt nun die Gleichung

$$(u-1)(u'y' - u') = p^b u'(u'-1)(y-1).$$

Daher gilt

j) $(u-1)(y'-1) = p^b(u'-1)(y-1)$.

Wäre $u = 1$, so wäre nach b) auch $t = 1$, dh., es wäre $N = \{1\}$. Dieser Widerspruch zeigt, dass $u > 1$ ist. Wäre $y = 1$, so wäre $t = u$ und aus b) folgte wiederum $t = 1$. Also ist auch $y > 1$. Daher folgt aus j), dass genau dann $y' = 1$ ist, wenn $u' = 1$ ist. Also folgt $t' = 1$ sowohl aus $y' = 1$ als auch aus $u' = 1$, da ja $t' = y'u'$ ist. Wir dürfen daher annehmen, dass u', $y' \neq 1$ ist. Dann ist aber

k) $(p^b u' - 1)(a' - 1)^{-1} = p^b(p^c y' - 1)(y' - 1)^{-1}$.

Wäre $b = 0$, so folgt aus k) auch $c = 0$, woraus mit d) der Widerspruch $0 = b + c = a \geq 1$ folgte. Also ist $b \neq 0$. Wegen $u' > 1$ ist

$$p^b - 1 \geq (p^b - 1)(u' - 1)^{-1}.$$

Daher ist

$$2p^b - 1 \geq b^b + (p^b - 1)(u' - 1)^{-1} = (p^b u' - 1)(u' - 1)^{-1}.$$

Wegen k) ist also

$$2p^b - 1 \geq p^b(p^c y' - 1)(y' - 1)^{-1}.$$

Folglich ist

$$2 > (p^c y' - 1)(y' - 1)^{-1} = p^c + (p^c - 1)(y' - 1)^{-1} \geq p^c,$$

so dass $c = 0$ ist. Aus j) folgt weiter, dass $p^b u' - 1 = p^b(u' - 1)$ ist. Hieraus folgt schließlich der Widerspruch $-1 \equiv 0 \bmod p$, so dass also doch $u' = 1 = y'$ ist.

Dies besagt wiederum, dass $t = p^a$ ist, womit gezeigt ist, dass N eine p-Gruppe ist.

Die Formel b) erhält nun die Gestalt

l) $k + (v-k)p^{-a} = 1 + (v-1)p^{-b}$.

Weil T ein projektiver Blockplan ist, ist $k(k-1) = \lambda(v-1)$. Ferner ist nach l)

$$\lambda(v-1) = \lambda p^b\bigl(k + (v-k)p^{-a} - 1\bigr),$$

so dass also $k(k-1) = \lambda p^b((v-k)p^{-a} + k - 1)$ ist. Somit ist $\lambda(v-k)p^{-a}$ und wegen $c \leq a$ dann auch $\lambda(v-k)p^{-c}$ durch $k-1$ teilbar. Wir definieren e durch

m) $\lambda(v-k)p^{-c} = e(k-1)$.

Multipliziert man 1) mit λp^b und beachtet man, dass $\lambda(v-1) = k(k-1)$ ist, so erhält man

$$k(k-1) = \lambda p^b(k-1) + \lambda(v-k)p^{-c}.$$

Hieraus und aus m) erhält man nun

n) $k = \lambda p^b + e$.

Aus f) folgt schließlich, dass

$$e - 1 = k - 1 - \lambda p^b = du - \lambda p^b = p^b(d-\lambda)$$

ist. Folglich ist $f := d - \lambda$ eine nicht negative ganze Zahl. Überdies ist

o) $e = p^b f + 1$.

Aus $k(k-1) = \lambda(v-1)$ folgt $\lambda(v-k) = (k-\lambda)(k-1)$. Mit m) erhält man daher $k = ep^c + \lambda$. Hieraus und aus o) folgt $k = fp^a + p^c + \lambda$. Wäre $f = 0$, so wäre $d = \lambda$, dh., es wäre $e = 1$. Aus m) und n) folgte daher $\lambda(v-k) = p^c\lambda p^b$ und somit $v - k = p^a = |N|$, so dass N auf $\Pi - c$ transitiv wäre. Dieser Widerspruch zeigt, dass $f \neq 0$ ist. Dann ist aber

p) $k > p^a$.

Weil $y = p^b > 1$ ist, ist c der einzige Fixblock von N. Sind nun P und Q zwei verschiedene Punkte auf c und sind $c = c_1, c_2, \ldots, c_\lambda$ alle Blöcke durch P und Q, so folgt, da die Stabilisatoren von $c_1, \ldots, c_\lambda$ alle in G konjugiert sind, dass es p-Gruppen N_i gibt, die c_i und nur c_i zum Fixblock haben. Wegen $N_i \subseteq G_{P,Q}$ für alle i ist $G_{P,Q}$ nach 7.10 auf $\{c_1, \ldots, c_\lambda\}$ transitiv. Hieraus folgt die Gleichung

$$|G_{P,Q} : G_{P,Q} \cap \Delta| = \lambda,$$

da ja $\Delta = G_c$ ist. Somit ist

$$|G_P : G_{P,Q} \cap \Delta| = |G_P : G_{P,Q}||G_{P,Q} : G_{P,Q} \cap \Delta| = \lambda(v-1) = k(k-1).$$

Weil G_P genau zwei Punktbahnen hat, hat G_P nach 3.4 auch genau zwei Blockbahnen. Folglich ist G_P auf der Menge der Blöcke durch P transitiv. Also ist $|G_P : G_P \cap \Delta| = k$. Hieraus folgt wiederum

$$\begin{aligned} k(k-1) &= |G_P : G_{P,Q} \cap \Delta| \\ &= |G_P : G_P \cap \Delta||G_P \cap \Delta : G_{P,Q} \cap \Delta| \\ &= k|G_P \cap \Delta : G_{P,Q} \cap \Delta|. \end{aligned}$$

Also ist $|G_P \cap \Delta : G_{P,Q} \cap \Delta| = k-1$, so dass $G_P \cap \Delta$ auf $c - \{P\}$ transitiv ist. Weil P ein beliebiger Punkt von c ist, operiert Δ auf c zweifach transitiv. Es sei nun $1 \neq \nu \in N$ und Z sei der Zentralisator von ν in G. Weil die Fixpunkte von ν gerade die Punkte von c sind, ist $c^z = c$, dh., es ist $Z \subseteq \Delta$. Nun ist $\nu^\Delta \subseteq N$, da N ein Normalteiler von Δ ist. Also ist

$$|\Delta : Z| \leq |N| = p^a,$$

so dass nach p) die Ungleichung $|\Delta : Z| < k$ gilt. Nach 11.2 ist Z folglich transitiv auf c. Nun hat ν genau k Fixpunkte. Daher hat ν nach 3.2 auch genau k Fixblöcke. Es seien $c_1 := c$, c_2, ..., c_k diese Fixblöcke. Weil Z auf c transitiv operiert, ist $(c, \{c_1, \ldots, c_k\}, \in)$ eine linksseitige taktische Konfiguration mit k Punkten. Weil nach 2.6 die Gleichung $|c_1 \cap c_i| = \lambda$ gilt für $i := 2, 3, \ldots, k$, folgt aus 1.2 a) die Kongruenz $k + \lambda(k-1) \equiv 0 \bmod k$. Hieraus folgt wiederum $\lambda \equiv 0 \bmod k$, so dass wegen $1 \leq \lambda \leq k$ sogar $k = \lambda$ gilt. Dann ist aber wegen $k(k-1) = \lambda(v-1)$ auch $k = v$. Dieser letzte Widerspruch zeigt schließlich, dass N doch auf $\Pi - c$ transitiv operiert.

Wir zeigen nun, dass G auf der Menge der nicht inzidenten Punkt-Geradenpaare von T transitiv operiert. Weil G zweifach transitiv ist, genügt es zu zeigen, dass der Stabilisator G_h einer Geraden h auf $\Pi - h$ noch transitiv ist. Es seien $c_1, \ldots, c_\lambda$ die Blöcke, die h enthalten. Ist dann N_i die Untergruppe von G, die c_i punktweise festlässt, so ist N_i auf $\Pi - c$ transitiv. Außerdem ist $N_i \subseteq G_h$. Weil

$$\Pi - h = \bigcup_{i:=1}^{\lambda} (\Pi - c_i)$$

ist, folgt, dass $\Pi - h$ eine Bahn von G_h ist, es sei denn, es gibt zwei Indizes i und j mit $(\Pi - c_i) \cap (\Pi - c_j) = \emptyset$. Dann ist aber $\Pi = c_i \cup c_j$ und daher $v = 2k - \lambda$. Aus

$$k(k-1) = \lambda(v-1) = \lambda(2k - \lambda - 1)$$

folgt die Gleichung $(k-\lambda)^2 = k - \lambda$. Wegen $k > \lambda$ ist somit $k = \lambda + 1$, woraus wiederum $v = k+1$ folgt. Wie wir jedoch schon früher bemerkten, ist $v \geq k+2$, so dass $\Pi - h$ doch eine Bahn von G_h ist. Nach 10.2 gibt es folglich einen Vektorraum V mit $r := \mathrm{Rg}(V) \geq 3$, so dass T und $L(V)_{1,r-1}$ isomorph sind.

Nun ist N auf $\Pi - c$ transitiv. Hieraus folgt mit 7.1, dass N alle Elationen mit der Achse c enthält, was wiederum impliziert, dass G alle Elationen von $T = L(V)_{1,r-1}$ enthält. Somit gilt auch $\mathrm{PSL}(V) \subseteq G \subseteq \mathrm{P\Gamma L}(V)$. Damit ist der Satz von Ito bewiesen.

V.

Polaritäten

Von besonderem Interesse unter den Korrelationen projektiver Räume sind die involutorischen Korrelationen. Sie werden gemeinhin Polaritäten genannt. Ihrem Studium und dem Studium ihrer Zentralisatoren ist das vorliegende Kapitel gewidmet. Dieses Studium werden wir in diesem Kapitel jedoch noch nicht beenden. Den orthogonalen Gruppen, die in diesen Kontext gehören, werden wir ein eigenes Kapitel widmen.[2]

1. Darstellung von Polaritäten

Es sei V ein K-Vektorraum mit $\mathrm{Rg}_K(V) \geq 3$. Eine Korrelation π von $\mathrm{L}(V)$ heißt *Polarität*, falls $\pi^2 = 1$ ist.

Wenn wir sagen, dass π eine Korrelation von $\mathrm{L}(V)$ sei, so beinhaltet das implizit, dass der Rang von V endlich ist, da $\mathrm{L}(V)$ ja höchstens in diesem Fall eine Korrelation gestattet, wie wir früher sahen.

1.1. Satz. *Es sei V ein Vektorraum über dem Körper K mit $\mathrm{Rg}(V) \geq 3$ und π sei eine Korrelation von $\mathrm{L}(V)$. Ferner werde π durch die α-Semibilinearform f dargestellt. Genau dann ist π eine Polarität, wenn aus u, $v \in V$ und $f(u,v) = 0$ stets $f(v,u) = 0$ folgt.*

Beweis. Wir definieren g durch $g(u,v) := f(v,u)^{\alpha^{-1}}$. Dann ist g nach II.8.7 eine α^{-1}-Semibilinearform und diese Form stellt π^{-1} dar. Nach II.8.8b) gilt daher genau dann $\pi^{-1} = \pi$, dh. $\pi^2 = 1$, wenn es ein $k \in K^*$ gibt mit $kg(u,v) = f(u,v)$ für alle u, $v \in V$. Ist $\pi^2 = 1$, so folgt also $f(v,u) = 0$ aus $f(u,v) = 0$.

Folgt andererseits $f(v,u) = 0$ aus $f(u,v) = 0$, so ist offensichtlich $U \leq U^{\pi^2}$ für alle $U \in \mathrm{L}(V)$. Weil V endlichen Rang hat, folgt $U = U^{\pi^2}$, so dass $\pi^2 = 1$ ist. Damit ist alles bewiesen.

1.2. Satz. *Es sei V ein Vektorraum über K mit $\mathrm{Rg}_K(V) \geq 3$. Wird die Polarität π von $\mathrm{L}(V)$ durch die α-Semibilinearform f dargestellt und gibt es einen Vektor $w \in V$ mit $f(w,w) = 1$, so ist $\alpha^2 = 1$ und $f(u,v) = f(v,u)^\alpha$ für alle u, $v \in V$.*

Beweis. Wie wir beim Beweise von 1.1 gesehen haben, gibt es ein $k \in K^*$ mit $f(u,v) = kf(v,u)^\alpha$ für alle u, $v \in V$. Es folgt

$$1 = f(w,w) = kf(w,w)^\alpha = k,$$

[2] Anmerkung der Herausgeber: Dieses Kapitel über orthogonale Gruppen fehlt.

so dass also tatsächlich $f(u,v) = f(v,u)^\alpha$ ist für alle u, $v \in V$.

Weil $f(u,v) = f(v,u)^\alpha$ ist für alle u und v, ist auch $f(v,u) = f(u,v)^\alpha$ für alle u, $v \in V$. Somit ist $f(u,v) = f(u,v)^{\alpha^2}$ für alle u, $v \in V$. Hieraus folgt

$$x = f(w,w)x = f(w,wx) = f(w,wx)^{\alpha^2} = f(w,w)^{\alpha^2} x^{\alpha^2} = x^{\alpha^2},$$

so dass $\alpha^2 = 1$ ist. Damit ist alles bewiesen.

Wir nennen die α-Semibilinearform f *symmetrisch*, falls $f(u,v) = f(v,u)^\alpha$ für alle u, $v \in V$ gilt. Wie wir gerade gesehen haben, ist dann $f(u,v) = f(u,v)^{\alpha^2}$. Gibt es Vektoren u, v mit $f(u,v) \neq 0$, so gibt es auch Vektoren u, v mit $f(u,v) = 1$. Dann ist aber

$$x = f(u,v)x = f(u,vx) = f(u,vx)^{\alpha^2} = f(u,v)^{\alpha^2} x^{\alpha^2} = x^{\alpha^2}$$

für alle $x \in K$, so dass $\alpha^2 = 1$ ist. Ist also f nicht die Nullform und ist f symmetrisch, so ist $\alpha^2 = 1$.

In Abschnitt 4 von Kapitel II hatten wir die Begriffe *absoluter Punkt* und *absolute Hyperebene* in Bezug auf eine Korrelation definiert. Wir wiederholen hier diese Definition für den Fall, dass π eine Polarität des projektiven Verbandes L ist. Ist P ein Punkt von L, so heißt P *absoluter Punkt* von π, falls $P \leq P^\pi$ ist. Analog heißt die Hyperebene H von L *absolut*, falls $H^\pi \leq H$ ist.

1.3. Satz. *Es sei V ein K-Vektorraum mit $\mathrm{Rg}_K(V) \geq 3$ und π sei eine Polarität von V. Sind nicht alle Punkte von $\mathrm{L}(V)$ absolut, so lässt sich π durch eine symmetrische α-Semibilinearform darstellen.*

Beweis. Nach dem dritten Struktursatz (II.8.3) gibt es eine β-Semibilinearform g, welche π darstellt. Da nicht alle Punkte absolut sind, gibt es ein $w \in V$ mit $g(w,w) \neq 0$. Setze $k := g(w,w)$ und definiere f durch $f(u,v) := k^{-1}g(u,v)$. Dann stellt auch f nach II.8.7a) die Polarität π dar. Wegen $f(w,w) = 1$ ist f nach 1.2 und der dem Beweise von 1.2 nachfolgenden Definition symmetrisch.

Der nächste Satz gibt Auskunft, was geschieht, wenn alle Punkte der Polarität π absolut sind.

1.4. Satz. *Es sei V ein K-Vektorraum mit $\mathrm{Rg}_K(V) \geq 3$. Ferner sei π eine Korrelation von $\mathrm{L}(V)$ und f eine π darstellende α-Semibilinearform. Sind alle Punkte von $\mathrm{L}(V)$ absolut bezüglich π, so gilt:*
a) *Es ist $f(v,v) = 0$ für alle $v \in V$.*
b) *Es ist $f(u,v) = -f(v,u)$ für alle u, $v \in V$.*
c) *π ist eine Polarität.*
d) *Es ist $\alpha = 1$. Insbesondere ist K kommutativ.*

Beweis. a) Ist $v = 0$, so ist $f(v,v) = 0$. Ist $v \neq 0$, so ist vK ein Punkt und daher $vK \leq (vK)^\pi$. Es folgt $f(v,v) = 0$.

b) Nach a) ist

$$0 = f(u+v,u+v) = f(u,u) + f(u,v) + f(v,u) + f(v,v) = f(u,v) + f(v,u),$$

woraus $f(u,v) = -f(v,u)$ folgt.

c) Wegen $f(u,v) = -f(v,u)$ ist $f(v,u) = 0$ eine Folge von $f(u,v) = 0$. Daher ist π nach 1.1 eine Polarität.

d) Weil f nicht ausgeartet ist, gibt es Vektoren u und v mit $f(u,v) \neq 0$. Setze $k := f(u,v)$. Ist $x \in K$, so folgt

$$kx = f(u,v)x = f(u,vx) = -f(vx,u) = -x^\alpha f(v,u) = x^\alpha f(u,v) = x^\alpha k.$$

Somit ist $x^\alpha = kxk^{-1}$, so dass α ein Automorphismus von K ist. Weil α andererseits auch ein Antiautomorphismus von K ist, ist K kommutativ. Hieraus folgt schließlich $x^\alpha = x$, so dass α die Identität ist.

Ist κ eine Korrelation des projektiven Verbandes L, so ist κ nichts anderes als ein Isomorphismus von L auf L^d. Daher ist $\mathrm{Rg}(X) = \mathrm{KoRg}(X^\kappa)$, dh. es ist

$$\mathrm{Rg}(L) = \mathrm{KoRg}(X^\kappa) + \mathrm{Rg}(X^\kappa) = \mathrm{Rg}(X) + \mathrm{Rg}(X^\kappa)$$

für alle $X \in L$. Aus dieser Bemerkung folgt unmittelbar der nächste Satz.

1.5. Satz. *Es sei V ein Vektorraum und κ sei eine Korrelation von* $\mathrm{L}(V)$. *Ist $X \in \mathrm{L}(V)$, so sind die folgenden Bedingungen äquivalent:*
a) *Es ist $X \cap X^\kappa = 0$.*
b) *Es ist $X + X^\kappa = V$.*
c) *Es ist $V = X \oplus X^\kappa$.*

Eine α-Semibilinearform mit $\alpha = 1$ nennen wir *Bilinearform*.

1.6. Satz. *Es sei V ein endlich erzeugter Vektorraum über K mit* $\mathrm{Rg}_K(V) \geq 2$ *und f sei eine nicht ausgeartete Bilinearform auf V. Ist $f(v,v) = 0$ für alle $v \in V$, so ist* $\mathrm{Rg}_K(V) = 2n$ *und es gibt eine Basis $b_1, \ldots, b_{2n}$ von V mit*

$$f\Big(\sum_{i:=1}^{2n} b_i x_i, \sum_{j:=1}^{2n} b_j y_j\Big) = \sum_{i:=1}^{n} (x_{2i-1}y_{2i} - x_{2i}y_{2i-1})$$

für alle n-Tupel x und y über K.

Beweis. Weil f nicht ausgeartet ist, gibt es Vektoren u, $v \in V$ mit $f(u,v) \neq 0$. Es gibt daher auch Vektoren b_1, $b_2 \in V$ mit $f(b_1,b_2) = 1$. Wären b_1 und b_2 linear abhängig, so wäre $b_2 = b_1 k$ mit einem $k \in K$ und daher

$$1 = f(b_1,b_2) = f(b_1,b_1)k = 0.$$

Dieser Widerspruch zeigt, dass b_1 und b_2 linear unabhängig sind. Gilt nun $\mathrm{Rg}_K(V) = 2$, so ist $\{b_1, b_2\}$ eine Basis von V und es ist, da ja offenbar $f(u,v) = -f(v,u)$ ist,

$$f(b_1x_1 + b_2x_2, b_1y_1 + b_2y_2) = x_1y_2 - x_2y_1.$$

Wir können daher annehmen, dass $\mathrm{Rg}_K(V) > 2$ ist. Weil f nicht ausgeartet ist, induziert f nach II.8.4 eine Korrelation π in $\mathrm{L}(V)$, die wegen $f(u,v) = -f(v,u)$ nach 1.1 sogar eine Polarität ist. Es sei $U := b_1K + b_2K$. Ist $v \in U \cap U^\pi$, so ist

$v = b_1x_1 + b_2x_2$ und $0 = f(b_1, v) = x_2$ und $0 = f(b_2, v) = x_1$, so dass $v = 0$ ist. Somit ist $U \cap U^\pi = \{0\}$. Nach 1.5 ist folglich $V = U \oplus U^\pi$. Weil $U^{\pi^2} = U$ ist, ist die Einschränkung von f auf U^π nicht ausgeartet. Nach Induktionsannahme ist daher $\mathrm{Rg}_K(U^\pi) = 2(n-1)$ und es gibt eine Basis $b_3, b_4, \ldots, b_{2n-1}, b_{2n}$ von U^π mit

$$f\big(\textstyle\sum_{i:=3}^{2n} b_ix_i, \sum_{j:=3}^{2n} b_jy_j\big) = \sum_{i:=2}^{n}(x_{2i-1}y_{2i} - x_{2i}y_{2i-1}).$$

Daher ist $\mathrm{Rg}_K(V) = 2n$ und

$$f\big(\textstyle\sum_{i:=1}^{2n} b_ix_i, \sum_{j:=1}^{2n} b_jy_j\big) = \sum_{i:=1}^{n}(x_{2i-1}y_{2i} - x_{2i}y_{2i-1}).$$

Damit ist alles bewiesen.

Ist π eine Polarität von $\mathrm{L}(V)$ und ist jeder Punkt von $\mathrm{L}(V)$ absolut, so nennen wir π *symplektisch*.

1.7. Satz. *Es sei V ein Vektorraum über K und es gelte* $\mathrm{Rg}_K(V) \geq 3$. *Genau dann besitzt* $\mathrm{L}(V)$ *eine symplektische Polarität, wenn K kommutativ und der Rang von V endlich und gerade ist. Sind π und π' symplektische Polaritäten von* $\mathrm{L}(V)$*, so gibt es ein* $\gamma \in \mathrm{PGL}(V)$ *mit* $\gamma^{-1}\pi\gamma = \pi'$.

Beweis. Besitzt $\mathrm{L}(V)$ eine symplektische Polarität, so folgt mit I.5.7, dass der Rang von V endlich ist. Aus 1.4 folgt die Kommutativität von K und aus 1.6, dass $\mathrm{Rg}_K(V)$ gerade ist.

Es sei umgekehrt $\mathrm{Rg}_K(V) = 2n$ und K sei kommutativ. Ist $b_1, \ldots, b_{2n}$ eine Basis von V und definiert man f durch

$$f\big(\textstyle\sum_{i:=1}^{2n} b_ix_i, \sum_{j:=1}^{2n} b_jy_j\big) := \sum_{i:=1}^{n}(x_{2i-1}y_{2i} - x_{2i}y_{2i-1}),$$

so verifiziert man leicht, dass f eine nicht ausgeartete Bilinearform mit $f(v, v) = 0$ für alle $v \in V$ ist, so dass $\mathrm{L}(V)$ nach II.8.4 und 1.4 eine symplektische Polarität besitzt.

Es seien schließlich π und π' symplektische Polaritäten von $\mathrm{L}(V)$. Ferner seien f und f' Bilinearformen, die π bzw. π' darstellen. Nach 1.4 und 1.6 gibt es dann Basen $b_1, \ldots, b_{2n}$ bzw. $b'_1, \ldots, b'_{2n}$ von V mit

$$f\big(\textstyle\sum_{i:=1}^{2n} b_ix_i, \sum_{j:=1}^{2n} b_jy_j\big) := \sum_{i:=1}^{n}(x_{2i-1}y_{2i} - x_{2i}y_{2i-1})$$

bzw.

$$f'\big(\textstyle\sum_{i:=1}^{2n} b'_ix_i, \sum_{j:=1}^{2n} b'_jy_j\big) := \sum_{i:=1}^{n}(x_{2i-1}y_{2i} - x_{2i}y_{2i-1}).$$

Es gibt ein $\beta \in \mathrm{GL}(V)$ mit $b_i^\beta = b'_i$ für $i := 1, \ldots, 2n$. Dann ist aber $f(u, v) = f'(u^\beta, v^\beta)$ für alle $u, v \in V$. Daher ist genau dann $v \in U^\pi$, wenn $v^\beta \in U^{\beta\pi'}$ ist. Andererseits ist genau dann $v \in U^\pi$, wenn $v^\beta \in U^{\pi\beta}$ ist. Folglich ist $U^{\pi\beta} = U^{\beta\pi'}$ für alle $U \in \mathrm{L}(V)$. Ist γ die von β in $\mathrm{L}(V)$ induzierte Kollineation, so ist also $\pi\gamma = \gamma\pi'$. Es folgt $\pi' = \gamma^{-1}\pi\gamma$, womit auch die letzte noch ausstehende Behauptung bewiesen ist.

Der gerade bewiesene Satz gibt Anlass für eine Definition. Ist π eine symplektische Polarität von $\mathrm{L}(V)$ und ist f eine π darstellende Bilinearform, ist ferner $b_1, \ldots, b_{2n}$ eine Basis von V mit

$$f\big(\sum_{i:=1}^{2n} b_i x_i, \sum_{j:=1}^{2n} b_j y_j\big) = \sum_{i:=1}^{n}(x_{2i-1}y_{2i} - x_{2i}y_{2i-1}),$$

so nennen wir $b_1, \ldots, b_{2n}$ eine *symplektische Basis* von V.

1.8. Satz. *Es sei V ein Vektorraum über K mit $\mathrm{Rg}_K(V) \geq 3$. Genau dann besitzt $\mathrm{L}(V)$ eine Polarität, wenn $\mathrm{Rg}_K(V)$ endlich ist und wenn K einen Antiautomorphismus α mit $\alpha^2 = 1$ besitzt.*

Beweis. Es sei π eine Polarität von V. Nach I.5.7 ist dann $\mathrm{Rg}_K(V)$ wegen $\mathrm{Rg}_K(V) = \mathrm{Rg}(\mathrm{L}(V))$ endlich. Ist π eine symplektische Polarität, so ist K kommutativ, und die Identität ist ein Antiautomorphismus von K. Ist π nicht symplektisch, so lässt sich π nach 1.3 mittels einer symmetrischen α-Semibilinearform darstellen. Nach der Bemerkung vor 1.3 ist dann $\alpha^2 = 1$.

Es sei umgekehrt $\mathrm{Rg}_K(V) = n$ endlich und α sei ein Antiautomorphismus von K mit $\alpha^2 = 1$. Ist $b_1, \ldots, b_n$ eine Basis von V, ist $u = \sum_{i:=1}^{n} b_i x_i$ und $v = \sum_{i:=1}^{n} b_n y_n$, so setzen wir

$$f(u, v) := \sum_{i:=1}^{n} x_i^\alpha y_i.$$

Man verifiziert mühelos, dass f eine symmetrische, nicht ausgeartete α-Semibilinearform ist, so dass $\mathrm{L}(V)$ nach II.8.4 und 1.1 eine Polarität besitzt.

Aus 1.8 folgt insbesondere, dass alle projektiven Geometrien endlichen Ranges, deren Koordinatenkörper kommutativ ist, Polaritäten besitzen, da ja in diesem Falle die Identität die Rolle des Antiautomorphismus α mit $\alpha^2 = 1$ spielen kann.

Es sei π eine Korrelation und f eine π darstellende α-Semibilinearform. Ist g eine ebenfalls π darstellende β-Semibilinearform, so gibt es nach II.8.7 ein Element $k \in K^*$ mit $x^\beta = k^{-1}x^\alpha k$ für alle $x \in K$. Ist nun $\alpha = 1$, so ist K kommutativ, so dass auch $\beta = 1$ ist. Hieraus folgt, dass jede π darstellende Semibilinearform eine Bilinearform ist, falls nur eine von ihnen es ist. Ist dies der Fall, so nennen wir die Korrelation π *projektiv*. Symplektische Polaritäten sind also stets projektiv. Nicht projektive Polaritäten heißen *unitär*.

Wie wir gesehen haben, lässt sich jede nicht symplektische Polarität π durch eine symmetrische α-Semibilinearform darstellen und im Falle, dass π projektiv ist, folgt aus II.8.7, dass alle π darstellenden Bilinearformen symmetrisch sind. Für unitäre Polaritäten gibt es noch eine Darstellungen durch eine *antisymmetrische* Semibilinearform, die gelegentlich von Nutzen ist. Hier die genaue Formulierung.

1.9. Satz. *Es sei V ein Vektorraum über K mit $\mathrm{Rg}_K(V) \geq 3$. Ferner sei π eine unitäre Polarität von $\mathrm{L}(V)$ und f sei eine π darstellende, symmetrische α-Semibilinearform. Es sei $l \in K$ und es gelte $l^\alpha \neq l$. Setze $k := l - l^\alpha$ und definiere β durch $x^\beta := kx^\alpha k^{-1}$. Setze schließlich*

$$g(u, v) := kf(u, v)$$

für alle u, $v \in V$. Dann ist g eine π darstellende β-Semibilinearform und es gilt

$$g(u,v) = -g(v,u)^\beta$$

für alle u, $v \in V$. Außerdem gilt $\beta^2 = 1$.

Beweis. Dass g eine β-Semibilinearform ist, die π darstellt, folgt mit II.8.7a). Dass $\beta^2 = 1$ ist, ist einfach nachzurechnen.

Es ist

$$k^\alpha = l^\alpha - l^{\alpha^2} = l^\alpha - l = -k$$

und

$$k^\beta = kk^\alpha k^{-1} = -kkk^{-1} = -k = k^\alpha,$$

so dass auch $k^\beta = -k$ gilt. Sind nun u, $v \in V$, so ist also

$$g(u,v) = kf(u,v) = kf(v,u)^\alpha k^{-1}k = -f(v,u)^\beta k^\beta = -(kf(u,v))^\beta = -g(v,u)^\beta.$$

Damit ist alles bewiesen.

2. Zentralisatoren von Polaritäten

Von großem geometrischem und algebraischem Interesse sind die Zentralisatoren von Polaritäten. Das geometrische Interesse an diesen Gruppen rührt daher, dass man mit ihrer Hilfe viel über die Struktur eines projektiven Raumes mit vorgegebener Polarität herausfinden kann, während das Interesse der Algebraiker an diesen Gruppen daher kommt, dass viele unter den Zentralisatoren von Polaritäten einfach sind, bzw. große einfache Untergruppen enthalten. In diesem Abschnitt beginnen wir das Studium dieser Gruppen.

2.1. Satz. *Es sei V ein Vektorraum über K mit $\mathrm{Rg}_K(V) \geq 3$ und κ sei eine Korrelation von $\mathrm{L}(V)$, die durch die α-Semibilinearform f dargestellt werde. Schließlich sei σ eine Kollineation von $\mathrm{L}(V)$ und β sei der begleitende Automorphismus von σ. (Wir interpretieren hier σ einmal als Kollineation und einmal als die sie induzierende semilineare Abbildung.) Genau dann ist $\kappa\sigma = \sigma\kappa$, wenn es ein $r \in K^*$ gibt, so dass $f(x^\sigma, y^\sigma) = rf(x,y)^\beta$ ist für alle x, $y \in V$.*

Beweis. Es sei $\kappa\sigma = \sigma\kappa$. Wir definieren g durch $g(x,y) := f(x^\sigma, y^\sigma)^{\beta^{-1}}$ für alle x, $y \in V$. Dann ist g eine $\beta\alpha\beta^{-1}$-Semibilinearform. Weil f nicht ausgeartet ist, ist auch g nicht ausgeartet. Daher stellt g nach II.8.4 eine Korrelation κ' dar. Nun ist

$$\begin{aligned} U^{\kappa'} &= \{v \mid v \in V, g(u,v) = 0 \text{ für alle } u \in U\} \\ &= \{v \mid v \in V, f(u^\sigma, v^\sigma) = 0 \text{ für alle } u \in U\}. \end{aligned}$$

Ersetzt man in dem letzten Ausdruck u und v durch $u^{\sigma^{-1}}$ bzw. $v^{\sigma^{-1}}$, so folgt weiter

$$\begin{aligned} U^{\kappa'} &= \{v^{\sigma^{-1}} \mid v \in V, f(u,v) = 0 \text{ für alle } u \in U^\sigma\} \\ &= \{v \mid v \in V, f(u,v) = 0 \text{ für alle } u \in U^\sigma\}^{\sigma^{-1}} = U^{\sigma\kappa\sigma^{-1}}. \end{aligned}$$

Hieraus folgt schließlich, da σ mit κ vertauschbar ist, dass $U^{\kappa'} = U^{\kappa}$ ist. Da dies für alle U gilt, ist $\kappa' = \kappa$. Weil κ also auch durch g dargestellt wird, gibt es nach II.8.7b) ein $s \in K^*$ mit $g(x,y) = sf(x,y)$ für alle x, $y \in V$. Setzt man schließlich $r := s^{\beta}$, so folgt $f(x^{\sigma}, y^{\sigma}) = rf(x,y)^{\beta}$.

Es sei umgekehrt $r \in K^*$ und es gelte $f(x^{\sigma}, y^{\sigma}) = rf(x,y)^{\beta}$. Dann ist genau dann $f(x,y) = 0$, wenn $f(x^{\sigma}, y^{\sigma}) = 0$ ist. Hieraus folgt

$$\begin{aligned} U^{\kappa\sigma} &= \bigl\{v^{\sigma} \mid v \in V, f(u,v) = 0 \text{ für alle } u \in U\bigr\} \\ &= \bigl\{v^{\sigma} \mid v \in V, f(u^{\sigma}, v^{\sigma}) = 0 \text{ für alle } u \in U\bigr\} \\ &= \bigl\{v \mid v \in V, f(u^{\sigma}, v) = 0 \text{ für alle } iu \in U\bigr\} \\ &= \bigl\{v \mid v \in V, f(u,v) = 0 \text{ für alle } u \in U^{\sigma}\bigr\} = U^{\sigma\kappa}, \end{aligned}$$

so dass $\kappa\sigma = \sigma\kappa$ ist. Damit ist alles bewiesen.

Ist π eine Polarität von $\mathrm{L}(V)$, so bezeichnen wir mit $PC^*(\pi)$ den Zentralisator von π in $\mathrm{PGL}(V)$ und mit $C^*(\pi)$ das volle Urbild von $PC^*(\pi)$ in $\mathrm{GL}(V)$.

2.2. Satz. *Es sei V ein Vektorraum über K mit $\mathrm{Rg}_K(V) \geq 3$ und π sei eine Polarität von $\mathrm{L}(V)$, die durch die α-Semibilinearform f dargestellt werde. Ist $\sigma \in C^*(\pi)$, so gibt es ein $r_{\sigma} \in K^*$ mit*

$$f(x^{\sigma}, y^{\sigma}) = r_{\sigma} f(x,y)$$

für alle x, $y \in V$. Die Abbildung r ist ein Homomorphismus von $C^*(\pi)$ in $Z(K^*)$, der von der Wahl von f unabhängig ist.

Beweis. Es sei $a \in K$. Dann ist

$$\begin{aligned} a^{\alpha} r_{\sigma} f(x,y) &= a^{\alpha} f(x^{\sigma}, y^{\sigma}) = f(x^{\sigma} a, y^{\sigma}) \\ &= f\bigl((xa)^{\sigma}, y^{\sigma}\bigr) = r_{\sigma} f(xa, y) = r_{\sigma} a^{\alpha} f(x,y). \end{aligned}$$

Weil f nicht ausgeartet ist, folgt $a^{\alpha} r_{\sigma} = r_{\sigma} a^{\alpha}$ für alle $a \in K$, so dass $r_{\sigma} \in Z(K^*)$ ist. Hieraus folgt weiter, dass

$$r_{\sigma\tau} f(x,y) = f(x^{\sigma\tau}, y^{\sigma\tau}) = r_{\tau} r_{\sigma} f(x,y) = r_{\sigma} r_{\tau} f(x,y).$$

Wiederum weil f nicht ausgeartet ist, folgt $r_{\sigma\tau} = r_{\sigma} r_{\tau}$, so dass r in der Tat ein Homomorphismus von $C^*(\pi)$ in $Z(K^*)$ ist.

Es bleibt zu zeigen, dass r nicht von f abhängt. Es sei also g eine zweite, π darstellende Semibilinearform. Nach II.8.7b) gibt es ein $k \in K^*$ mit $g(x,y) = kf(x,y)$ für alle x, $y \in V$. Ist $\sigma \in C^*(\pi)$, so ist also, da ja $r_{\sigma} \in Z(K)$ gilt,

$$g(x^{\sigma}, y^{\sigma}) = kf(x^{\sigma}, y^{\sigma}) = kr_{\sigma} f(x,y) = r_{\sigma} kf(x,y) = r_{\sigma} g(x,y),$$

so dass r in der Tat nicht von der Darstellung von π abhängt.

Den Kern der Abbildung r bezeichnen wir mit $C(\pi)$. Er besteht aus allen Abbildungen $\sigma \in \mathrm{GL}(V)$ mit $f(x^{\sigma}, y^{\sigma}) = f(x,y)$ für alle x, $y \in V$. Die Elemente aus $C(\pi)$ heißen auch *Isometrien* des Paares (V, π). Die von $C(\pi)$ in $\mathrm{L}(V)$

induzierte Kollineationsgruppe bezeichnen wir mit $PC(\pi)$. Sie ist normal in $PC^*(\pi)$.

2.3. Satz. *Es sei V ein Vektorraum über K und π sei eine Polarität von* $\mathrm{L}(V)$. *Ferner sei r der in 2.2 beschriebene Homomorphismus von $C^*(\pi)$ in $Z(K^*)$. Wird π durch die α-Semibilinearform f dargestellt und ist $\sigma \in C^*(\pi)$, so ist $r_\sigma^\alpha = r_\sigma$.*

Beweis. Ist $\alpha = 1$, so ist nichts zu beweisen. Es sei also $\alpha \neq 1$. Dann ist π nach Satz 1.4d) nicht symplektisch. Nach 1.3 gibt es folglich eine symmetrische β-Semibilinearform g, die π darstellt. Für g und β gilt daher, da r_σ im Zentrum von K liegt,

$$\begin{aligned} g(x,y)r_\sigma = r_\sigma g(x,y) &= g(x^\sigma, y^\sigma) = g(y^\sigma, x^\sigma)^\beta \\ &= \big(r_\sigma g(y,x)\big)^\beta = g(y,x)^\beta r_\sigma^\beta = g(x,y) r_\sigma^\beta. \end{aligned}$$

Weil g nicht ausgeartet ist, folgt $r_\sigma = r_\sigma^\beta$. Nun unterscheiden sich α und β nach II.8.7a) nur um einen inneren Automorphismus von K, so dass auch $r_\sigma = r_\sigma^\alpha$ gilt, da r_σ ja im Zentrum von K liegt.

2.4. Satz. *Ist π eine Polarität des projektiven Verbandes* $\mathrm{L}(V)$, *so ist der Quotient $PC^*(\pi)/PC(\pi)$ eine elementarabelsche 2-Gruppe.*

Beweis. Es sei $\sigma \in C^*(\pi)$ und f sei eine π darstellende α-Semibilinearform. Wir definieren ρ durch $v^\rho := v r_\sigma^{-1}$ für $v \in V$. Dann ist, da ja $r_\sigma^\alpha = r_\sigma \in Z(K)$ gilt,

$$f(u^{\sigma^2\rho}, v^{\sigma^2\rho}) = r_\sigma^{-\alpha} f(u^{\sigma^2}, v^{\sigma^2}) r_\sigma^{-1} = r_\sigma^{-2} r_\sigma^2 f(u,v) = f(u,v).$$

Somit ist $\sigma^2\rho \in C(\pi)$. Weil σ^2 und $\sigma^2\rho$ in $\mathrm{L}(V)$ die gleiche Kollineation induzieren, folgt, dass $PC^*(\pi)/PC(\pi)$ eine elementarabelsche 2-Gruppe ist.

In einigen Fällen können wir noch weitergehende Aussagen machen.

2.5. Satz. *Ist V ein Vektorraum mit $\mathrm{Rg}_K(V) \geq 3$ über dem endlichen Körper K und ist π eine unitäre Polarität von* $\mathrm{L}(V)$, *so ist $PC^*(\pi) = PC(\pi)$.*

Beweis. Weil π nicht symplektisch ist, gibt es eine symmetrische α-Semibilinearform f, die π darstellt. Insbesondere ist dann $\alpha^2 = 1$ jedoch $\alpha \neq 1$. Hieraus folgt, dass $K = \mathrm{GF}(q^2)$ ist und dass für alle $k \in K$ die Gleichung $k^\alpha = k^q$ gilt.

Es sei $\sigma \in C^*(\pi)$. Dann ist $f(u^\sigma, v^\sigma) = r_\sigma f(u,v)$ für alle u, $v \in V$. Wegen $r_\sigma^\alpha = r_\sigma$ ist $r_\sigma \in \mathrm{GF}(q)$ und aus $K^{q+1} = \mathrm{GF}(q)$ folgt die Existenz eines $a \in K^*$ mit $r_\sigma = a^{q+1} = a^{\alpha+1}$. Wir definieren ρ durch $v^\rho := va^{-1}$ für alle $v \in V$. Dann ist

$$f(u^{\sigma\rho}, v^{\sigma\rho}) = a^{-\alpha} f(u^\sigma, v^\sigma) a^{-1} = a^{-\alpha-1} r_\sigma f(u,v) = f(u,v),$$

so dass $\sigma\rho \in C(\pi)$ ist. Weil σ und $\sigma\rho$ in $\mathrm{L}(V)$ die gleiche Kollineation induzieren, folgt $PC^*(\pi) = PC(\pi)$, q. e. d.

2.6. Satz. *Es sei V ein Vektorraum über K mit $\mathrm{Rg}_K(V) \geq 3$. Ist π eine symplektische Polarität von* $\mathrm{L}(V)$, *so ist der in 2.2 definierte Homomorphismus*

r surjektiv. Insbesondere ist also $C^*(\pi)/C(\pi) \cong K^*$ und $PC^*(\pi)/PC(\pi) \cong K^*/K^{*2}$.

Beweis. Es sei f eine π darstellende Bilinearform. Nach 1.7 ist $\mathrm{Rg}_K(V) = 2n$ und nach 1.6 besitzt V eine symplektische Basis $b_1, \ldots, b_{2n}$. Für $a \in K^*$ definieren wir die Abbildung $\sigma \in \mathrm{GL}(V)$ vermöge $b_{2i-1}^\sigma := -b_{2i}$ und $b_{2i}^\sigma := b_{2i-1}a$ für $i := 1, \ldots, n$. Eine leichte, wenn auch längliche Rechnung — man nehme ein Blatt in Querformat — zeigt, dass $f(u^\sigma, v^\sigma) = af(u,v)$ ist. Folglich ist $\sigma \in C^*(\pi)$ und $r_\sigma = a$. Dies zeigt die Surjektivität von r. Hieraus folgt unmittelbar die vorletzte Aussage des Satzes.

Um die letzte Aussage zu beweisen, sei $\sigma \in C^*(\pi)$ und N bezeichne den Kern des Homomorphismus P von $C^*(\pi)$ auf $PC^*(\pi)$. Wir setzen

$$\varphi(\sigma N) := r_\sigma K^{*2}.$$

Ist $\tau \in \sigma N$, so ist $v^{\sigma\tau^{-1}} = va$ für alle $v \in V$ mit einem von v unabhängigem $a \in K^*$. Es folgt

$$r_\sigma r_\tau^{-1} f(u,v) = r_{\sigma\tau^{-1}} f(u,v) = f(u^{\sigma\tau^{-1}}, v^{\sigma\tau^{-1}}) = f(ua, va) = a^2 f(u,v)$$

Also ist $r_\sigma = r_\tau a^2$, so dass τ wohldefiniert ist. Nach dem bereits Bewiesenen ist φ surjektiv.

Genau dann ist $\varphi(\sigma N) = K^{*2}$, wenn $r_\sigma = k^2$ ist mit einem $k \in K^*$. Insbesondere ist also $PC(\pi) \subseteq \mathrm{Kern}(\varphi)$. Es sei $\sigma N \in \mathrm{Kern}(\varphi)$. Dann ist $r_\sigma = k^2$. Definiere τ durch $v^\tau := v^\sigma k^{-1}$. Dann ist

$$f(u^\tau, v^\tau) = k^{-2} f(u^\sigma, v^\sigma) = k^{-2} r_\sigma f(u,v) = f(u,v)$$

für alle u, $v \in V$. Es folgt $\sigma N = \tau N \in PC(\pi)$. Damit ist alles gezeigt.

2.7. Satz. *Es sei V ein Vektorraum des Ranges $n \geq 3$ über dem kommutativen Körper K. Ferner sei π eine Polarität von $\mathrm{L}(V)$, die durch die α-Semibilinearform f dargestellt werde. Ist $\sigma \in C^*(\pi)$, so gibt es ein $a \in K^*$ mit $r_\sigma^n = a^{\alpha+1}$.*

Beweis. Es sei $b_1, \ldots, b_n$ eine Basis von V und F sei die durch $F_{ij} := f(b_i, b_j)$ definierte Matrix. Ferner sei c die durch $b_i^\sigma := \sum_{r:=1}^n b_r c_{ri}$ definierte Matrix. Schließlich sei $a := \det(F)$. Dann ist

$$r_\sigma f(b_i, b_j) = f(b_i^\sigma, b_j^\sigma) = f\left(\sum_{r:=1}^n b_r c_{ri}, \sum_{s:=1}^n b_s c_{sj}\right) = \sum_{r:=1}^n \sum_{s:=1}^n c_{ri}^\alpha f(b_r, b_s) c_{sj}.$$

Also ist $r_\sigma F = c^{\alpha t} F c$ — t bedeutet transponieren. Daher ist

$$r_\sigma^n \det(F) = \det(c^\alpha)\det(c)\det(F).$$

Nun ist f nicht ausgeartet, woraus folgt, dass $\det(F) \neq 0$ ist. Somit ist $r_\sigma^n = \det(c)^\alpha \det(c) = a^{\alpha+1}$, q. e. d.

2.8. Satz. *Es sei V ein Vektorraum über dem kommutativen Körper K mit $\mathrm{Rg}_K(V) \geq 3$, und π sei eine Polarität von $\mathrm{L}(V)$, die von der α-Semibilinearform*

f dargestellt werde. Ist der Rang von V ungerade, so ist $C^*(\pi)/C(\pi) \cong (K^*)^{1+\alpha}$ und daher $PC^*(\pi) = PC(\pi)$.

Beweis. Setze $n := \mathrm{Rg}_K(V)$. Dann ist $n = 2k+1$. Nach 2.7 gilt $r_\sigma^n = a^{\alpha+1}$ mit einem $a \in K^*$. Wir setzen $b := r_\sigma^{-k}$. Nach 2.3 ist dann $b^\alpha = b$. Folglich ist

$$r_\sigma = r_\sigma^{2k+1} b^2 = a^{\alpha+1} b^\alpha b = (ab)^{\alpha+1}.$$

Dies besagt, dass r ein Homomorphismus von $C^*(\pi)$ in $(K^*)^{1+\alpha}$ ist. Weil andererseits $(K^*)^{\alpha+1}$ im Bild von r enthalten ist, folgt, dass r ein Epimorphismus von $C^*(\pi)$ auf $(K^*)^{\alpha+1}$ ist. Ist nun $\sigma \in C^*(\pi)$, so gibt es also ein $c \in K^*$ mit $r_\sigma = c^{\alpha+1}$. Definiert man ρ vermöge $v^\rho := vc^{-1}$ für alle $v \in V$, so folgt $\sigma\rho \in C(\pi)$. Weil σ und $\sigma\rho$ die gleiche Kollineation in $\mathrm{L}(V)$ hervorrufen, ist daher $PC^*(\pi) = PC(\pi)$. Damit ist alles bewiesen.

2.9. Satz. *Es sei K ein endlicher Körper und Q sei die Menge der Quadrate von K. Sind a und b zwei von 0 verschiedene Elemente von K, so ist $K = aQ + bQ$.*

Beweis. Ist die Charakteristik von K gleich 2, so ist $K = Q$ und weiter nichts zu beweisen. Es sei also die Charakteristik von K von 2 verschieden. Dann enthält K^* genau $\frac{1}{2}(q-1)$ Quadrate, so dass Q wegen $0^2 = 0$ genau $\frac{1}{2}(q+1)$ Elemente enthält. Ist nun $k \in K$, so gelten wegen a, $b \neq 0$ die Gleichungen

$$|aQ| = \frac{1}{2}(q+1) = |-bQ+k|.$$

Somit ist

$$\begin{aligned} q \geq \big|(aQ) \cup (-bQ+k)\big| &= |aQ| + |-bQ+k| - \big|(aQ) \cap (-bQ+k)\big| \\ &= q + 1 - \big|(aQ) \cap (-bQ+k)\big|. \end{aligned}$$

Hieraus folgt, dass $(aQ) \cap (-bQ+k) \neq \emptyset$ ist. Es gibt also Elemente g, $h \in Q$ mit $ag = -bh + k$, so dass $k = ag + bh$ ist.

2.10. Satz. *Es sei V ein Vektorraum geraden Ranges über dem endlichen Körper K. Ist π eine projektive Polarität von $\mathrm{L}(V)$, so ist $C^*(\pi)/C(\pi) \cong K^*$ und daher $PC^*(\pi)/PC(\pi) \cong K^*/K^{*2}$.*

Beweis. Dies ist nach 2.6 richtig, falls π symplektisch ist. Ist die Charakteristik von K gleich 2, so ist jedes Element von K ein Quadrat. Weil das Bild von r die Gruppe der Quadrate umfasst, folgt auch in diesem Falle, dass $C^*(\pi)/C(\pi) \cong K^*$ ist, was wiederum $PC^*(\pi)/PC(\pi) \cong K^*/K^{*2}$ nach sich zieht. Wir dürfen daher annehmen, dass π nicht symplektisch ist und dass die Charakteristik von K von 2 verschieden ist.

Weil π nicht symplektisch ist, gibt es einen Punkt P mit $P \not\leq P^\pi$. Nach 1.5 ist daher $V = P \oplus P^\pi$. Es sei f eine π darstellende symmetrische Bilinearform. Wäre $f(u,u) = 0$ für alle $u \in P^\pi$, so wäre

$$0 = f(u+u', u+u') = 2f(u,u')$$

für alle u, $u' \in P^\pi$. Weil die Charakteristik von K von 2 verschieden ist, ist daher $f(u,u') = 0$ für alle u, $u' \in P^\pi$. Ist $v \in V$, so ist $v = p + u$ mit $p \in P$ und $u \in P^\pi$. Ist $x \in P^\pi$, so folgt

$$f(x,v) = f(x,p+u) = f(x,p) + f(x,u) = 0.$$

Da dies für alle $v \in V$ gilt, folgt $x = 0$, da f ja nicht ausgeartet ist. Also ist $P^\pi = \{0\}$ und somit $V = P$. Dieser Widerspruch zeigt, dass es einen Punkt $Q \leq P^\pi$ gibt, der nicht absolut ist. Es sei $G := P + Q$ und $P = pK$ sowie $Q = qK$. Indem man f notfalls mit einem Skalarfaktor abändert — Hier benutzen wir, dass r nicht von der Auswahl von f abhängt —, kann man erreichen, dass $f(p,p) = 1$ ist. Ist $x := pk + ql \in G \cap G^\pi$, so ist $0 = f(p,x) = k$ und $0 = f(q,x) = f(q,q)l$, so dass $k = l = 0$ ist. Also ist $G \cap G^\pi = \{0\}$ und daher $V = G \oplus G^\pi$.

Es sei $s \in K^*$ und s sei kein Quadrat.

1. Fall: Es sei $f(q,q)$ kein Quadrat. Dann ist $sf(q,q)$ ein Quadrat. Es gibt also Elemente b, $c \in K^*$ mit $s = c^2 f(q,q)$ und $sf(q,q) = b^2$. Setze ferner $a := 0$ und $d := 0$.

2. Fall: Es sei $f(q,q)$ ein Quadrat. In diesem Falle dürfen wir annehmen, dass $f(q,q) = 1$ ist. Nach 2.9 gibt es Elemente a, $c \in K$ mit $s = a^2 + c^2$. In diesem Falle setzen wir $b := c$ und $d := -a$.

Wir definieren nun eine Abbildung σ' auf G vermöge $p^{\sigma'} := pa + qc$ und $q^{\sigma'} := pb + qd$. Dann ist, wie leicht nachzurechnen, $f(g^{\sigma'}, h^{\sigma'}) = sf(g,h)$ für alle g, $h \in G$. Wegen $\mathrm{Rg}_K(V) = 2 + \mathrm{Rg}_K(G^\pi)$ ist auch $\mathrm{Rg}_K(V^\pi)$ gerade. Es gibt daher nach Induktionsannahme eine Abbildung $\sigma'' \in \mathrm{GL}(G^\pi)$ mit $f(u^{\sigma''}, v^{\sigma''}) = sf(u,v)$ für alle u, $v \in G^\pi$. Ist schließlich $v \in V$ und $v = x + y$ mit $x \in G$ und $y \in G^\pi$ und definiert man σ durch $v^\sigma := x^{\sigma'} + x^{\sigma''}$, so zeigt eine triviale Rechnung, dass $f(u^\sigma, v^\sigma) = sf(u,v)$ für alle u, $v \in V$ ist. Da die Quadrate stets im Bilde von r liegen, ist damit gezeigt, dass r surjektiv ist.

3. Symplektische Polaritäten und ihre Zentralisatoren

Ist π eine symplektische Polarität von $\mathrm{L}_K(V)$, so setzen wir $\mathrm{Sp}(V) := C(\pi)$ und $\mathrm{PSp}(V) := PC(\pi)$. Soll der Rang aus irgendeinem Grunde erwähnt werden, so schreiben wir statt $\mathrm{Sp}(V)$ und $\mathrm{PSp}(V)$ auch $\mathrm{Sp}(n,K)$ bzw. $\mathrm{PSp}(n,K)$. Diese Bezeichnungsweisen sind gerechtfertigt, da die Struktur von $\mathrm{Sp}(V)$ und $\mathrm{PSp}(V)$ nach 1.7 nur von V abhängt. Ist f eine Form, die π darstellt, so ist f also eine nicht ausgeartete, alternierende Bilinearform und $\mathrm{Sp}(V)$ ist die Gruppe aller $\sigma \in \mathrm{GL}(V)$ mit $f(u^\sigma, v^\sigma) = f(u,v)$ für alle u, $v \in V$. Wir nennen beide Gruppen, $\mathrm{Sp}(V)$ und $\mathrm{PSp}(V)$ *symplektisch*.

3.1. Satz. *Es sei V ein Vektorraum geraden Ranges über dem kommutativen Körper K. Ist $\sigma \in \mathrm{GL}(V)$, so sind die folgenden Aussagen äquivalent:*
a) *Es ist $\sigma \in \mathrm{Sp}(V)$.*
b) *Symplektische Basen werden von σ auf symplektische Basen abgebildet.*
c) *Es gibt eine symplektische Basis, die von σ auf eine symplektische Basis abgebildet wird.*

Ferner ist die Gruppe $\mathrm{Sp}(V)$ *auf der Menge der symplektischen Basen scharf transitiv.*

Beweis. Ist $b_1, \ldots, b_{2n}$ eine Basis von V, so ist

$$f(b_{2i-1}, b_{2i}) = 1 = -f(b_{2i}, b_{2i-1})$$

für $i := 1, \ldots, n$ und $f(b_i, b_j) = 0$ für alle übrigen Indexpaare kennzeichnend dafür, dass $b_1, \ldots, b_{2n}$ eine symplektische Basis von V ist. Dabei ist f eine Bilinearform, die eine symplektische Polarität darstellt. Ist $\sigma \in \mathrm{Sp}(V)$, so ist also mit $b_1, \ldots, b_{2n}$ auch $b_1^\sigma, \ldots, b_{2n}^\sigma$ eine symplektische Basis. Es ist also b) eine Folge von a).

Da es nach 1.6 stets symplektische Basen gibt, ist c) eine Folge von b).

Es sei $\sigma \in \mathrm{GL}(V)$ und $b_1, \ldots, b_{2n}$ und $b_1^\sigma, \ldots, b_{2n}^\sigma$ seien symplektische Basen von V. Ist $u = \sum_{i:=1}^{2n} b_i x_i$ und $v = \sum_{i:=1}^{2n} b_i y_i$, so ist folglich

$$f(u, v) = \sum_{i:=1}^{n} (x_{2i-1} y_{2i} - x_{2i} y_{2i-1})$$

und

$$f(u^\sigma, v^\sigma) = \sum_{i:=1}^{n} (x_{2i-1} y_{2i} - x_{2i} y_{2i-1}),$$

so dass $f(u^\sigma, v^\sigma) = f(u, v)$ ist. Dies besagt aber gerade, dass σ ein Element der symplektischen Gruppe ist. Also ist a) eine Folge von c).

Sind schließlich $b_1, \ldots, b_{2n}$ und $c_1, \ldots, c_{2n}$ zwei symplektische Basen von V, so gibt es genau ein $\sigma \in \mathrm{GL}(V)$ mit $b_i^\sigma = c_i$ für alle i, so dass $\mathrm{Sp}(V)$ nach dem bereits Bewiesenen auf der Menge der symplektischen Basen scharf transitiv operiert. Damit ist alles bewiesen.

3.2. Satz. *Es sei* V *ein Vektorraum über dem kommutativen Körper* K *und* f *sei eine nicht ausgeartete, alternierende Bilinearform auf* V. *Sind dann* $\{b_1, b_3, \ldots, b_{2r+1}\}$ *und* $\{b_2, b_4, \ldots, b_{2s}\}$ *Mengen von linear unabhängigen Vektoren mit*

$$f(b_{2i-1}, b_{2i}) = 1 = -f(b_{2i}, b_{2i-1})$$

für $i := 1, \ldots, \min\{r, s\}$ *sowie* $f(b_i, b_j) = 0$ *für alle übrigen Indexpaare, so gibt es eine symplektische Basis* $c_1, \ldots, c_{2n}$ *mit* $c_{2i-1} = b_{2i-1}$ *für* $i := 1, \ldots, r$ *und* $c_{2i} = b_{2i}$ *für* $i := 1, \ldots, s$.

Beweis. Wir dürfen annehmen, dass weder $\{b_1, \ldots, b_{2r+1}\}$ noch $\{b_2, \ldots, b_{2s}\}$ leer ist. Sind nämlich beide Mengen leer, so besagt der Satz nichts anderes als die Existenz von symplektischen Basen. Ist eine der beiden Mengen, etwa die zweite, leer, so ist

$$b_3 K + b_5 K + \ldots b_{2r+1} K < b_1 K + b_3 K + \ldots b_{2r+1} K,$$

so dass also

$$(b_1 K + b_3 K + \ldots b_{2r+1} K)^\pi < (b_3 K + b_5 K + \ldots b_{2r+1} K)^\pi$$

ist. Dabei bezeichne π die von f induzierte symplektische Polarität. Es gibt also einen Vektor $y \in (b_3K + \ldots + b_{2r+1}K)^\pi$, der nicht in $(b_1K + \ldots b_{2r+1}K)^\pi$ liegt. Setze $b_2 := f(b_1, y)^{-1}y$. Dann ist $f(b_1, b_2) = 1$ und $f(b_{2i+1}, b_2) = 0$ für $i := 1, \ldots, r$. Damit ist die Zwischenbehauptung bewiesen.

Ist nun $\mathrm{Rg}_K(V) = 2$, so ist b_1, b_2 eine symplektische Basis von V, so dass der Satz in diesem Falle bewiesen ist. Es sei also $\mathrm{Rg}_K(V) > 2$. Nun ist $G := b_1K + b_2K$ eine Gerade von $\mathrm{L}(V)$ mit $V = G \oplus G^\pi$, wie wir schon einmal bemerkten. Auf Grund unserer Annahme gilt

$$\{b_3, \ldots, b_{2r+1}\} \cup \{b_4, \ldots, b_{2s}\} \subseteq G^\pi.$$

Wegen $\mathrm{Rg}_K(G) = \mathrm{Rg}_K(V) - 2$ führt Induktion zum Ziele.

Statt $\mathrm{Sp}(2n, \mathrm{GF}(q))$ bzw. $\mathrm{PSp}(2n, \mathrm{GF}(q))$ schreiben wir im Folgenden auch $\mathrm{Sp}(2n, q)$ bzw. $\mathrm{PSp}(2n, q)$. Man beachte, dass der Rang eines projektiven Geometrie mit einer symplektischen Polarität stets gerade ist.

3.3. Satz. *Es ist*

$$\big|\mathrm{Sp}(2n, q)\big| = q^{n^2} \prod_{i:=1}^{n} (q^{2i} - 1)$$

und

$$\big|\mathrm{PSp}(2n, q)\big| = \frac{1}{\mathrm{ggT}(2, q-1)} \big|\mathrm{Sp}(2n, q)\big|.$$

Beweis. Weil $\mathrm{Sp}(2n, q)$ auf den symplektischen Basen des zugehörigen Vektorraumes scharf transitiv operiert, ist $|\mathrm{Sp}(2n, q)|$ gleich der Anzahl dieser Basen. Ist $b_1, b_2, \ldots, b_{2n}$ eine symplektische Basis von V, so ist $b_3, \ldots, b_{2n}$ eine symplektische Basis von $(b_1K + b_2K)^\pi$, so dass die Anzahl der symplektischen Basen von V gleich der Anzahl der Paare b_1, b_2 mit $f(b_1, b_2) = 1$ mal der Anzahl der symplektischen Basen eines Vektorraumes vom Range $2n - 2$ ist. Ist nun b_1 ein vom Nullvektor verschiedener Vektor und ist xK ein Punkt, der nicht in $(b_1K)^\pi$ liegt, so ist $f(b_1, x) \neq 0$. Es gibt also genau ein $b_2 \in xK$ mit $f(b_1, b_2) = 1$. Die Anzahl der Vektoren b_2 mit $f(b_1, b_2) = 1$ ist somit gleich der Anzahl der Punkte von $\mathrm{L}(V)$, die nicht in der Hyperebene $(b_1K)^\pi$ liegen, dh. gleich q^{2n-1}. Folglich ist die Anzahl der Paare b_1, b_2 gleich $(q^{2n} - 1)q^{2n-1}$. Daher ist die Anzahl der symplektischen Basen von V gleich

$$(q^{2n} - 1)q^{2n-1}q^{(n-1)^2} \prod_{i:=1}^{n-1} (q^{2i} - 1).$$

Also ist

$$\big|\mathrm{Sp}(2n, q)\big| = q^{n^2} \prod_{i:=1}^{n} (q^{2i} - 1).$$

Ist σ im Kern des Homomorphismus von $\mathrm{Sp}(2n, q)$ auf $\mathrm{PSp}(2n, q)$, so ist $v^\sigma = vk$ für alle $v \in V$ und einem geeigneten $k \in K^*$. Es folgt $f(u, v) = f(u^\sigma, v^\sigma) =$

$f(u,v)k^2$ und weiter $k^2 = 1$. Also ist $k = 1$ oder $k = -1$. Hieraus folgt auch noch die letzte Behauptung des Satzes.

Es sei π eine Polarität von $\mathrm{L}(V)$. Ist $U \in \mathrm{L}(V)$ und gilt $U \cap U^\pi \neq \{0\}$, so heißt U *isotrop*. Ist sogar $U \leq U^\pi$, so heißt U *vollständig isotrop*. Ist U vollständig isotrop, so ist

$$2\mathrm{Rg}_K(U) \leq \mathrm{Rg}_K(U) + \mathrm{Rg}_K(U^\pi) = \mathrm{Rg}_K(V)$$

und daher $\mathrm{Rg}_K(U) \leq \frac{1}{2}\mathrm{Rg}_K(V)$.

3.4. Satz. *Es sei V ein Vektorraum des Ranges $2n$ über dem kommutativen Körper K und π sei eine symplektische Polarität von $\mathrm{L}(V)$. Ist $U \in \mathrm{L}(V)$ vollständig isotrop, so gibt es einen vollständig isotropen Unterraum W von V mit $U \leq W$ und $W = W^\pi$, dh. mit $\mathrm{Rg}_K(W) = n$.*

Beweis. Es sei $\mathrm{Rg}_K(U) = r + 1$ und $b_1, b_3, \ldots, b_{2r+1}$ sei eine Basis von U. Weil U vollständig isotrop ist, erfüllen dann $\{b_1, b_3, \ldots, b_{2r+1}\}$ und $\emptyset$ die Voraussetzungen von 3.2. Es gibt daher eine symplektische Basis $c_1, c_2, \ldots, c_{2n}$ von V mit $b_{2i+1} = c_{2i+1}$ für $i := 0, \ldots, r$. Setze $W := \sum_{i:=1}^{n} c_{2i-1}K$. Dann ist $U \leq W$ und $W = W^\pi$, q. e. d.

3.5. Satz. *Es sei V ein Vektorraum und π sei eine symplektische Polarität von $\mathrm{L}(V)$. Ferner seien $U, W \in \mathrm{L}(V)$. Genau dann gibt es ein $\sigma \in \mathrm{Sp}(V)$ mit $U^\sigma = W$, wenn $\mathrm{Rg}_K(U) = \mathrm{Rg}_K(W)$ und $\mathrm{Rg}_K(U \cap U^\pi) = \mathrm{Rg}_K(W \cap W^\pi)$ ist.*

Beweis. Ist $\sigma \in \mathrm{Sp}(V)$ und ist $U^\sigma = W$, so folgt aus $\sigma\pi = \pi\sigma$, dass $U^{\pi\sigma} = W^\pi$ ist. Folglich ist auch $(U \cap U^\pi)^\sigma = W \cap W^\pi$, so dass in der Tat $\mathrm{Rg}_K(U) = \mathrm{Rg}_K(W)$ und $\mathrm{Rg}_K(U \cap U^\pi) = \mathrm{Rg}_K(W \cap W^\pi)$ ist.

Es sei umgekehrt $\mathrm{Rg}_K(U) = \mathrm{Rg}_K(W)$ und $\mathrm{Rg}_K(U \cap U^\pi) = \mathrm{Rg}_K(W \cap W^\pi)$. Ist nun $U = U_0 \oplus (U \cap U^\pi)$ und $W = W_0 \oplus (W \cap W^\pi)$, so ist also $\mathrm{Rg}_K(U_0) = \mathrm{Rg}_K(W_0)$ und U_0 und W_0 sind beide nicht isotrop. Es gibt also symplektische Basen $b_1, \ldots, b_{2s}$ von U_0 bzw. $b'_1, \ldots, b'_{2s}$ von W_0. Es sei ferner $b_{2s+1}, b_{2s+3}, \ldots, b_{2r+1}$ eine Basis von $U \cap U^\pi$ und $b'_{2s+1}, b'_{2s+3}, \ldots, b'_{2r+1}$ eine solche von $W \cap W^\pi$. Dann erfüllen $\{b_1, b_3, \ldots, b_{2r+1}\}$ und $\{b_2, b_4, \ldots, b_{2s}\}$ bzw. $\{b'_1, b'_3, \ldots, b_{2r+1}\}$ und $\{b'_2, b'_4, \ldots, b'_{2s}\}$ die Voraussetzungen von 3.2, so dass aus diesem Satz und aus 3.1 die Existenz eines $\sigma \in \mathrm{Sp}(V)$ mit $U^\sigma = W$ folgt.

3.6. Satz. *Ist V ein Vektorraum des Ranges 2 über dem kommutativen Körper K, so ist $\mathrm{Sp}(V) = \mathrm{SL}(V)$ und somit auch $\mathrm{PSp}(V) = \mathrm{PSL}(V)$.*

Beweis. Es sei b_1, b_2 eine symplektische Basis von V und $\sigma \in \mathrm{GL}(V)$. Ist $b_i^\sigma = b_1 a_{1i} + b_2 a_{2i}$, so ist

$$f(b_1^\sigma, b_2^\sigma) = a_{11}a_{22} - a_{12}a_{21} = \det(\sigma).$$

Folglich ist b_1^σ, b_2^σ genau dann eine symplektische Basis von V, wenn $\det(\sigma) = 1$, dh. wenn $\sigma \in \mathrm{SL}(V)$ ist (Satz III.1.12b)). Aus 3.1 folgt daher die Behauptung.

3.7. Satz. *Es sei V ein Vektorraum über dem kommutativen Körper K und f sei eine nicht ausgeartete, alternierende Bilinearform auf V.*

a) *Ist* $a \in V$ *und* $k \in K$, *so liegt die durch* $x^\tau := x + af(a,x)k$ *definierte Transvektion* τ *in* $\mathrm{Sp}(V)$.

b) *Ist* φ *eine lineare Abbildung von* V *in* K, *ist ferner* $a \in \mathrm{Kern}(\varphi)$ *und liegt die durch* $x^\tau := x + a\varphi(x)$ *definierte Transvektion* τ *in* $\mathrm{Sp}(V)$, *so gibt es ein* $k \in K$ *mit* $\varphi(x) = f(a,x)k$ *für alle* $x \in V$.

Beweis. a) Es ist klar, dass die Abbildung $x \to f(a,x)k$ linear ist, da K ja kommutativ ist. Wegen $f(a,a) = 0$ ist τ folglich eine Transvektion. Schließlich ist

$$f(x^\tau, y^\tau) = f(x,y) + f(x,a)f(a,y)k + f(a,y)f(a,x)k + f(a,a)f(a,x)f(a,y)k^2,$$

so dass wegen $f(a,a) = 0$ und $f(a,x) = -f(x,a)$ für alle x, $y \in V$ die Gleichung $f(x^\tau, y^\tau) = f(x,y)$ gilt. Folglich ist $\tau \in \mathrm{Sp}(V)$.

b) Wir dürfen annehmen, dass $\tau \neq 1$ ist. Dann ist aK das Zentrum der von τ induzierten Elation. Ist π die von f induzierte symplektische Polarität, so folgt aus $\pi\tau = \tau\pi$, dass $(aK)^\pi$ die Achse von τ ist. Daher ist

$$\mathrm{Kern}(\varphi) = (aK)^\pi = \big\{x \mid x \in V, f(a,x) = 0\big\}.$$

Hieraus folgt, dass es ein $k \in K$ gibt mit $\varphi(x) = f(a,x)k$ für alle $x \in V$. Damit ist der Satz bewiesen.

3.8. Satz. *Die Gruppe* $\mathrm{Sp}(2n,K)$ *wird von Transvektionen erzeugt. Insbesondere ist* $\det(\sigma) = 1$ *für alle* $\sigma \in \mathrm{Sp}(2n,K)$.

Beweis. Es sei T die von allen in $\mathrm{Sp}(2n,K)$ liegenden Transvektionen erzeugte Untergruppe von $\mathrm{Sp}(2n,K)$. Wir zeigen zunächst, dass T auf der Menge der von 0 verschiedenen Vektoren von V transitiv operiert. Es seien also a, b zwei von 0 verschiedene Vektoren aus V. Ist $f(a,b) \neq 0$, so gibt es ein $k \in K$ mit $f(a,b)k = -1$. Die durch

$$v^\tau := v + (b-a)f(b-a,v)k$$

definierte Transvektion liegt nach 3.7a) in T. Ferner ist

$$a^\tau = a + (b-a)f(b-a,a)k = a + (b-a)f(b,a)k = b$$

In diesem Falle gibt es also sogar eine Transvektion, die a auf b abbildet. Ist $f(a,b) = 0$, so gibt es einen Vektor c mit $f(a,c) \neq 0 \neq f(b,c)$. Nach dem eben Bewiesenen gibt es dann zwei Transvektionen σ, $\tau \in T$ mit $a^\sigma = c$ und $c^\tau = b$, so dass es auch in diesem Falle ein Element in T gibt, nämlich $\sigma\tau$, welches a auf b abbildet.

Es seien nun a, b und a', b' zwei Paare von Vektoren mit $f(a,b) = 1$ und $f(a',b') = 1$. Wir zeigen, dass es ein $\rho \in T$ gibt, mit $a^\rho = a'$ und $b^\rho = b'$. Weil T auf $V - \{0\}$ transitiv operiert, dürfen wir $a = a'$ annehmen. Ist $f(b',b) \neq 0$, so gibt es ein $k \in K$ mit $f(b',b)k = 1$. In diesem Falle definieren wir τ durch

$$x^\tau := x + (b'-b)f(b'-b,x)k.$$

Dann ist

$$\begin{aligned} a^\tau &= a + (b' - b)\big(f(b', a) - f(b, a)\big)k \\ &= a' + (b' - b)\big(f(b', a') - f(b, a)\big)k \\ &= a' + (b' - b)\big(-1 + 1\big)k = a' \end{aligned}$$

und

$$b^\tau = b + (b' - b)\big(f(b', b) - f(b, b)\big)k = b'.$$

Ist $f(b', b) = 0$, so betrachten wir die beiden Paare a, b und a, $a + b$ sowie a, $a + b$ und a, b'. Dann ist $f(b, a + b) = -1 \neq 0$ und $f(a + b, b') = f(a, b') = f(a', b') = 1 \neq 0$, so dass es zwei Transvektionen σ, $\tau \in T$ gibt mit $a^\sigma = a = a^\tau$ und $b^\sigma = a + b$ und $(a + b)^\tau = b'$. Es folgt $a^{\sigma\tau} = a'$ und $b^{\sigma\tau} = b'$.

Ist nun $n = 1$, so ist 3.8 wegen 3.6 richtig. Es sei also $n > 1$ und $\gamma \in \mathrm{Sp}(2n, K)$. Es gibt $a, b \in V$ mit $f(a, b) = 1$. Dann ist auch $f(a^\gamma, b^\gamma) = 1$, so dass es ein $\rho \in T$ gibt mit $a^{\gamma\rho} = a$ und $b^{\gamma\rho} = b$. Wegen $f(a, b) = 1$ ist $aK + bK$ nicht isotrop. Ist π die durch f induzierte symplektische Polarität und $U := aK + bK$, so ist also $V = U \oplus U^\pi$ und $U^{\pi\gamma\rho} = U^\pi$, da ja $\gamma\rho \in \mathrm{Sp}(2n, K)$. Wegen $\mathrm{Rg}_K(U^\pi) = 2(n - 1)$ gibt es dann Transvektionen $\lambda_1, \ldots, \lambda_r \in \mathrm{Sp}(2n - 2, K)$ mit $x^{\gamma\rho} = x^\sigma$ für alle $x \in U^\pi$, wobei $\sigma := \lambda_1 \cdots \lambda_r$ gesetzt wurde. Definiert man nun τ_i durch

$$(u + x)^{\tau_i} := u + x^{\lambda_i},$$

so ist τ_i eine Transvektion aus $\mathrm{Sp}(2n, K)$ und es ist $\gamma\rho = \tau_1 \cdots \tau_r$, so dass also $\gamma \in T$ gilt. Damit ist der Satz bewiesen.

Zur Erinnerung: Ist G eine Gruppe, so bezeichnen wir mit G' die Kommutatorgruppe von G.

3.9. Satz. *Ist K ein kommutativer Körper und n eine natürliche Zahl, so ist $\mathrm{Sp}(2n, K) = \mathrm{Sp}(2n, K)'$, es sei denn, es ist $n = 1$ und $|K| \leq 3$ oder $n = 2$ und $|K| = 2$.*

Beweis. Wir betrachten zunächst den Fall $|K| > 3$. Es gibt dann ein $k \in K$ mit $k^2 \neq 0, 1$. Es sei $0 \neq a \in V$. Es gibt dann ein $\sigma \in \mathrm{Sp}(2n, K)$ mit $a^\sigma = ak$. Es sei τ die durch $x^\tau := x + af(a, x)l$ mit $l \in K$ definierte Transvektion. Dann ist

$$\begin{aligned} x^{\sigma^{-1}\tau^{-1}\sigma\tau} &= \big(x^{\sigma^{-1}} - af(a, x^{\sigma^{-1}})l\big)^{\sigma\tau} \\ &= \big(x - a^\sigma f(a, x^{\sigma^{-1}})l\big)^\tau \\ &= \big(x - akf(a, x^{\sigma^{-1}})l\big)^\tau \\ &= x^\tau - a^\tau kf(a, x^{\sigma^{-1}})l \\ &= x + af(a, x)l - ak^2 f(a^{\sigma^{-1}}, x^{\sigma^{-1}})l. \end{aligned}$$

Weil $\sigma \in \mathrm{Sp}(2n, K)$ ist, ist $f(a^{\sigma^{-1}}, x^{\sigma^{-1}}) = f(a, x)$. Also ist

$$x^{\sigma^{-1}\tau^{-1}\sigma\tau} = x + af(a, x)(1 - k^2)l.$$

Da a irgendein Vektor ist und weil $1 - k^2 \neq 0$ ist, folgt mit 3.7, dass jede Transvektion aus $\mathrm{Sp}(2n, K)$ ein Kommutator ist. Weil $\mathrm{Sp}(2n, K)$ nach 3.8 von

ihren Transvektionen erzeugt wird, ist $\mathrm{Sp}(2n,K)$ also in diesem Falle gleich ihrer Kommutatorgruppe.

Als Nächstes betrachten wir den Fall $|K|=3$ und $n\geq 2$. Dann ist $\mathrm{Rg}_K(V)\geq 4$. Jede symplektische Basis hat also mindestens vier Vektoren. Es seien v_1, v_2, v_3, v_4 die ersten vier Vektoren einer solchen Basis. Setze $U := (\sum_{i:=1}^4 v_iK)^\pi$. Dann ist $V = (\sum_{i:=1}^4 v_iK)\oplus U$. Ferner ist auch $v_1,\ v_2+v_3,\ v_3,\ v_1+v_4$ eine symplektische Basis von $\sum_{i:=1}^4 v_iK$. Es gibt zwei Abbildungen $\sigma,\ \tau\in \mathrm{GL}(V)$ mit $v_1^\sigma = v_2,\ v_2^\sigma = -v_1,\ v_3^\sigma = v_3,\ v_4^\sigma = v_4$ und $u^\sigma = u$ für alle $u\in U$, bzw. $v_1^\tau = v_2+v_3,\ (v_2+v_3)^\tau = -v_1,\ v_3^\tau = v_3,\ (v_1+v_4)^\tau = v_1+v_4$ und wiederum $u^\tau = u$ für alle $u\in U$. Mit 3.1 erschließen wir, dass σ und τ in $\mathrm{Sp}(2n,K)$ liegen. Man rechnet ferner leicht nach, dass $\sigma^4=\tau^4=1$ ist. Nun wird $\mathrm{Sp}(2n,K)$ von Transvektionen erzeugt, die wegen $|K|=3$ alle die Ordnung 3 haben. Daher ist $\mathrm{Sp}(2n,K)/\mathrm{Sp}(2n,K)'$ eine elementarabelsche 3-Gruppe, so dass wegen $\sigma^4=\tau^4=1$ die Abbildungen σ und τ in $\mathrm{Sp}(2n,K)'$ liegen. Wir betrachten die Abbildung $(\tau\sigma)^2$. Es ist, wie eine einfache Rechnung zeigt, $v_i^{(\tau\sigma)^2} = v_i$ für $i := 1,\ 2,\ 3$. Ferner ist — hier benutzen wir, dass wegen $|K|=3$ die Gleichung $-v_3 = 2v_3$ gilt —,

$$\begin{aligned} v_4^{(\tau\sigma)^2} &= (v_1+v_4-v_1)^{(\tau\sigma)^2} = (v_1+v_4-v_2-v_3)^{\sigma\tau\sigma} \\ &= (v_2+v_4+v_1-v_3)^{\tau\sigma} = (v_2+v_3+v_1+v_4+v_3)^{\tau\sigma} \\ &= (-v_1+v_1+v_4+v_3)^{\sigma} = v_3+v_4. \end{aligned}$$

Schließlich ist $u^{(\tau\sigma)^2} = u$ für alle $u\in U$. Definiert man ρ durch $x^\rho := x + v_3f(v_3,x)$, so ist ρ eine Transvektion. Ferner sieht man, dass ρ mit $(\tau\sigma)^2$ auf der Menge $\{v_1,v_2,v_3,v_4\}\cup U$ übereinstimmt, so dass $\rho = (\tau\sigma)^2$ ist. Also ist $\rho\in \mathrm{Sp}(2n,K)'$.

Es sei nun τ eine Transvektion ungleich 1 aus $\mathrm{Sp}(2n,K)$. Nach 3.7 gibt es ein $a\in V$ und ein $k\in K$ mit $x^\tau = x + af(a,x)k$ für alle $x\in V$. Wegen $\tau\neq 1$ ist $a\neq 0$ und $k\neq 0$. Es gibt also ein $\lambda\in \mathrm{Sp}(2n,K)$ mit $a^\lambda = v_3$. Es folgt $x^{\lambda^{-1}\tau\lambda} = x + v_3f(a,x)k$. Wegen $k\neq 0$ und $|K|=3$ ist $k=1$ oder -1. Dies besagt, dass τ zu ρ oder ρ^{-1} konjugiert ist. Weil $\mathrm{Sp}(2n,K)'$ ein Normalteiler von $\mathrm{Sp}(2n,K)$ ist, folgt $\rho\in \mathrm{Sp}(2n,K)'$. Hieraus folgt wieder, dass $\mathrm{Sp}(2n,K) = \mathrm{Sp}(2n,K)'$ ist.

Schließlich sei $|K|=2$ und $n\geq 3$. In diesem Falle ist $\mathrm{Rg}_K(V)\geq 6$. Es gibt daher sechs Vektoren $v_1,\ \dots,\ v_6$, die den Anfang einer symplektischen Basis bilden. Wir setzen wieder $U := (\sum_{i:=1}^6 v_iK)^\pi$. Es folgt $V = (\sum_{i:=1}^6 v_iK)\oplus U$.

Wir definieren eine Abbildung $\rho\in \mathrm{Sp}(2n,K)$ vermöge $v_i^\rho := v_i$ für $i := 1$, 2, 5, 6 und $v_3^\rho := v_3+v_4$ und $v_4^\rho := v_3$ sowie $u^\rho := u$ für alle $u\in U$. (Dass ρ tatsächlich in $\mathrm{Sp}(2n,K)$ liegt, erschließt man wieder mit Satz 3.1.) Dann ist $\rho^3=1$. Weil $\mathrm{Sp}(2n,K)$ von Transvektionen erzeugt wird, die wegen $|K|=2$ die Ordnung 2 haben, ist $\mathrm{Sp}(2n,K)/\mathrm{Sp}(2n,K)'$ eine elementarabelsche 2-Gruppe. Folglich ist $\rho\in \mathrm{Sp}(2n,K)'$

Wir definieren eine weitere Abbildung $\sigma\in \mathrm{Sp}(2n,K)$ vermöge $v_i^\sigma := v_i$ für $i := 1,\ 5,\ 6$ sowie $(v_2+v_4)^\sigma = v_2+v_4$, $(v_1+v_3)^\sigma = v_4$ und $v_4^\sigma = v_1+v_3+v_4$ sowie $u^\sigma = u$ für alle $u\in U$. Dann ist $\sigma^3=1$, so dass auch $\sigma\in \mathrm{Sp}(2n,K)'$ gilt.

Folglich ist $\mu_1 := \rho\sigma \in \mathrm{Sp}(2n, K)'$. Man rechnet leicht nach, dass

$$v_1^{\mu_1} = v_1,\ v_3^{\mu_1} = v_3,\ v_5^{\mu_1} = v_5$$

und

$$v_2^{\mu_1} = v_1 + v_2 + v_3,\ v_4^{\mu_1} = v_1 + v_4,\ v_6^{\mu_1} = v_6$$

sowie $u^{\mu_1} = u$ für alle $u \in U$ ist. Ersetzt man hierin der Reihe nach v_1, v_2, v_3, v_4, v_5, v_6 durch v_1, v_2, v_5, v_6, v_3, v_4, so sieht man, dass es auch eine Abbildung $\mu_2 \in \mathrm{Sp}(2n, K)'$ gibt mit

$$v_1^{\mu_2} = v_1,\ v_5^{\mu_2} = v_5,\ v_3^{\mu_2} = v_3$$

und

$$v_2^{\mu_2} = v_1 + v_2 + v_5,\ v_6^{\mu_2} = v_1 + v_6,\ v_4^{\mu_2} = v_4$$

sowie $u^{\mu_2} = u$ für alle $u \in U$ ist. Ersetzt man wiederum in der ersten Gruppe von Gleichungen v_1, v_2, v_3, v_4, v_5, v_6 der Reihe nach durch v_1, v_2, $v_3 + v_5$, v_4, v_5, $v_4 + v_6$, so folgt, dass es ein $\mu_3 \in \mathrm{Sp}(2n, K)'$ gibt mit

$$v_1^{\mu_3} = v_1,\ v_3^{\mu_3} = v_3,\ v_5^{\mu_3} = v_5$$

und

$$v_2^{\mu_3} = v_1 + v_2 + v_3 + v_5,\ v_4^{\mu_3} = v_1 + v_4,\ v_6^{\mu_3} = v_1 + v_6$$

sowie $u^{\mu_3} = u$ für alle $u \in U$ ist. Setzt man nun $\mu := \mu_1\mu_2\mu_3$, so zeigen einfache Rechnungen, dass für $i \neq 2$ die Gleichung $v_i^\mu = v_i$ gilt, dass $v_2^\mu = v_1 + v_2$ und dass $u^\mu = u$ für alle $u \in U$ ist. Folglich ist μ eine in $\mathrm{Sp}(2n, K)'$ liegende, von 1 verschiedene Transvektion. Weil die Charakteristik von K gleich 2 ist, sind alle Transvektionen aus $\mathrm{Sp}(2n, K)$ konjugiert, so dass auch in diesem Falle $\mathrm{Sp}(2n, K) = \mathrm{Sp}(2n, K)'$ gilt. Damit ist der Satz bewiesen.

Die Gruppen $\mathrm{SL}(2, 2)$ und $\mathrm{SL}(2, 3)$ sind auflösbar, so dass im Falle $|K| \leq 3$ und $n = 1$ tatsächlich $\mathrm{Sp}(2, K)' \neq \mathrm{Sp}(2, K)$ ist. Dass auch $\mathrm{Sp}(4, 2)' \neq \mathrm{Sp}(4, 2)$ ist, werden wir am Ende dieses Abschnitts sehen, wo wir zeigen werden, dass $\mathrm{Sp}(4, 2)$ und S_6 isomorph sind.

3.10. Satz. *Es sei V ein Vektorraum über K und π sei eine symplektische Polarität von $\mathrm{L}(V)$. Ist $G := \mathrm{PSp}(V)$ die zugehörige projektive symplektische Gruppe, so gilt:*

a) *G ist auf der Menge der Punkte von $\mathrm{L}(V)$ transitiv.*

b) *Ist P ein Punkt von $\mathrm{L}(V)$, so hat G_P genau drei Punktbahnen, nämlich: $\{P\}$, die Menge der von P verschiedenen Punkte von P^π (diese Menge ist im Falle $\mathrm{Rg}_K(V) = 2$ leer) und die Menge der Punkte von $\mathrm{L}(V)_{P^\pi}$.*

c) *G operiert auf der Menge der Punkte von $\mathrm{L}(V)$ primitiv.*

Beweis. a) folgt aus der Transitivität von $\mathrm{Sp}(V)$ auf der Menge der von Null verschiedenen Vektoren von V.

b) Es sei $P = pK$. Ferner seien uK und vK zwei Punkte von P^π. Dann ist $f(p, u) = 0 = f(p, v)$. Aus 3.2 und 3.1 folgt die Existenz einer Abbildung

$\rho \in \mathrm{Sp}(V)$ mit $p^\rho = p$ und $u^\rho = v$, so dass die von P verschiedenen Punkte von P^π eine Bahn von G_P bilden.

Es seien uK und vK zwei Punkte, die nicht in P^π liegen. Dann ist $f(p,u)$, $f(p,v) \neq 0$. Wir dürfen daher, indem wir ggf. u und v durch skalare Vielfache ersetzen, annehmen, dass $f(p,u) = 1 = f(p,v)$ ist. Wiederum mit 3.2 und 3.1 erschließen wir die Existenz eines $\sigma \in \mathrm{Sp}(V)$ mit $p^\sigma = p$ und $u^\sigma = v$, so dass auch die Punkte außerhalb von P^π eine Bahn von G_P bilden.

Angenommen G sei imprimitiv. Ist Δ ein Imprimitivitätsgebiet von G, so ist also $|\Delta| \geq 2$, jedoch enthält Δ nicht alle Punkte von $\mathrm{L}(V)$. Es sei $P \in \Delta$. Ist $H := G_P$, so ist $\Delta^H = \Delta$. Folglich zerfällt Δ in genau zwei Bahnen von H. Aus b) folgt somit, dass Δ entweder aus den Punkten von P^π oder aus P und den Punkten des affinen Raumes $\mathrm{L}(V)_{P^\pi}$ besteht. Beides führt aber auf einen Widerspruch. Nach a) ist G ja auf den Punkten von $\mathrm{L}(V)$ transitiv. Weil nun jede Hyperebene von V von der Form P^π ist, wobei P ein Punkt ist, ist G auch auf der Menge der Hyperebenen transitiv. Folglich wären alle Hyperebenen Imprimitivitätsgebiete. Dies kann aber nicht sein, da Hyperebenen stets Punkte gemeinsam haben, Imprimitivitätsgebiete aber disjunkt liegen. Da es andererseits zu zwei verschiedene Hyperebenen stets einen Punkt gibt, der auf keiner der beiden Hyperebenen liegt, kann auch der zweite Fall nicht eintreten. Damit ist auch c) bewiesen.

3.11. Satz. *Die Gruppe* $\mathrm{PSp}(2n,K)$ *ist einfach, es sei denn es ist* $n = 1$ *und* $|K| \leq 3$ *oder* $n = 2$ *und* $|K| = 2$.

Beweis. Setze $G := \mathrm{PSp}(2n,K)$. Es sei P ein Punkt der zugrunde liegenden Geometrie. Die in G liegenden Elationen mit dem Zentrum P bilden einen abelschen Normalteiler A_P von G_P. Ist Q ein weiterer Punkt, so folgt mit 3.10a), dass A_P und A_Q in G konjugiert sind. Nach 3.8 wird G von seinen Elationen erzeugt. Nach 3.10c) operiert G auf der Punktmenge von $\mathrm{L}(V)$ primitiv und nach 3.8 ist $G = G'$, falls nicht einer der drei im Satz erwähnten Ausnahmefälle auftritt. Folglich ist G, von den Ausnahmefällen abgesehen, nach Satz III.2.1, dem Satz von Iwasawa, einfach.

Die Gruppen $\mathrm{PSp}(2,2)$ und $\mathrm{PSp}(2,3)$ sind, wie wir schon bemerkten, auflösbar. Dass auch $\mathrm{PSp}(4,2)$ nicht einfach ist, zeigt der folgende Satz.

3.12. Satz. *Die Gruppen* $\mathrm{PSp}(4,2)$ *und* S_6 *sind isomorph.*

Beweis. Wir betrachten die Menge $M := \{1,2,3,4,5,6\}$ und bezeichnen mit Π die Menge ihrer 2-Teilmengen. Ist $P \in \Pi$, so sei b_P die Menge aus P und den 2-Teilmengen von $M - P$. Schließlich sei $\Gamma := \{b_P \mid P \in \Pi\}$. Wir betrachten die Inzidenzstruktur

$$\Lambda := (\Pi, \Gamma, \in).$$

Die nächste Aussage folgt unmittelbar aus der Definition.

a) Sind P, $Q \in \Pi$, so ist genau dann $P \in b_Q$, wenn $P = Q$ oder $P \cap Q = \emptyset$ ist.

Aus a) folgt, dass die Anzahl r_P der Blöcke durch den Punkt P gleich $1 + \binom{4}{2} = 7$ und dass die Anzahl k_b von Punkten auf einem Block ebenfalls gleich

$1 + \binom{4}{2} = 7$ ist. Also ist Λ eine taktische Konfiguration mit den Parametern $v = b = \binom{6}{2} = 15$ und $r = k = 7$.

b) Es sei $P := \{a, b\}$ und $Q := \{a, c\}$ und $b \neq c$. Es sei ferner $X \in \Pi$. Genau dann ist $P, Q \in B_X$, wenn $P \cap X = \emptyset = Q \cap X$ ist.

Ist $P \cap X = Q \cap X = \emptyset$, so ist $P, Q \in b_X$ nach a). Es seien $P, Q \in b_X$. Wäre $P = X$, so folgte $a \in Q \cap X$. Mit a) folgt weiter $Q = X$ und damit $Q = P$ im Widerspruch zu $c \neq b$.

c) Sind $P, Q \in \Pi$ und ist $P \cap Q = \emptyset$, so sind b_P, b_Q und $b_{P-(P\cup Q)}$ die einzigen Blöcke, die gleichzeitig mit P und Q inzidieren.

Dies folgt unmittelbar aus a).

Aus b) und c) folgt, dass zwei verschiedene Punkte von Λ mit genau drei Blöcken inzidieren. Λ ist also ein 2-(15,7,3)-Blockplan.

Es seien P und Q zwei verschiedene Punkte von Λ. Mit $P + Q$ bezeichnen wir ihre Verbindungsgerade, das ist der Schnitt über die drei Blöcke, die P und Q enthalten. Ist $P \cap Q \neq \emptyset$, so gilt nach b) genau dann $Y \in P + Q$, wenn $Y \cap X = \emptyset$ ist für alle 2-Teilmengen X von $M - (P \cap Q)$, dh. genau dann, wenn Y eine 2-Teilmenge von $P \cup Q$ ist. In diesem Falle ist also $|P + Q| = 3$. Ist $P \cap Q = \emptyset$, so folgt aus c), dass P, Q und $M - (P \cup Q)$ die einzigen Punkte auf $P + Q$ sind. Also gilt auch in diesem Falle $|P + Q| = 3$. Nun ist

$$\frac{b - \lambda}{r - \lambda} = \frac{15 - 3}{7 - 3} = 3,$$

so dass $(\Pi, \Gamma, \in)$ nach IIII.10.1 die Geometrie aus den Punkten und Ebenen der projektiven Geometrie L des Ranges 4 über GF(2) ist. Ferner folgt, dass S_6 eine Kollineationsgruppe von L ist. Wir definieren nun π durch $P^\pi := b_P$ und $b_P^\pi := P$. Weil genau dann $P \in b_Q$ gilt, wenn $P = Q$ oder $P \cap Q = \emptyset$ ist, und da dies mit $Q = P$ und $Q \cap P = \emptyset$ gleichbedeutend ist, gilt genau dann $P \in b_Q$, wenn $Q \in b_P$ gilt. Daher ist π eine Polarität, die wegen $P \in b_P = P^\pi$ symplektisch ist. Es folgt $S_6 \subseteq PC^*(\pi)$. Weil L eine projektiver Raum über GF(2) ist, gilt $PC^*(\pi) = PC(\pi) = \mathrm{PSp}(4, 2)$ nach 2.6. Also ist sogar $S_6 \subseteq \mathrm{PSp}(4, 2)$. Aus 3.3 folgt schließlich, dass $|\mathrm{PSp}(4, 2)| = 6! = |S_6|$ ist, so dass in der Tat $S_6 = \mathrm{PSp}(4, 2)$ gilt.

4. Polaritäten bei Charakteristik 2

Die Zentralisatoren von Polaritäten operieren in der Regel irreduzibel auf den zugrunde liegenden Vektorräumen. Ausnahmen treten nur bei Charakteristik 2 auf. Einen der zwei möglichen Ausnahmefälle wollen wir in diesem Abschnitt betrachten. Der hier nicht behandelte Fall ist der einer unitären Polarität π von $\mathrm{L}(V)$.

Im Folgenden sei V ein Vektorraum über dem Körper K der Charakteristik 2 und es sei $\mathrm{Rg}_K(V) \geq 3$. Ferner sei π eine projektive Polarität von $\mathrm{L}(V)$ und f sei eine π darstellende Bilinearform. Wie wir wissen, ist f symmetrisch. Sind $u, v \in V$, so ist

$$f(u + v, u + v) = f(u, u) + 2f(u, v) + f(v, v) = f(u, u) + f(v, v).$$

Hieraus folgt, dass die Menge

$$H := \{v \mid v \in V, f(v,v) = 0\}$$

ein Unterraum von V ist. Wir nehmen weiterhin an, dass π nicht symplektisch ist. Dann ist also $H \neq V$.

4.1. Satz. *Es sei V ein Vektorraum des Ranges mindestens 3 über dem kommutativen Körper K der Charakteristik 2. Ferner sei π eine projektive Polarität von $\mathrm{L}(V)$, die nicht symplektisch sei. Ist dann f eine π darstellende Bilinearform und setzt man*

$$H := \{v \mid v \in V, f(v,v) = 0\},$$

so ist $1 \leq \mathrm{Rg}_K(V/H) \leq [K : K^2]$. Insbesondere ist H eine Hyperebene, falls K perfekt ist.

Beweis. Weil H von V verschieden ist, ist der Rang von V/H mindestens 1. Die Abbildung $v \to f(v,v)$ ist eine semilineare Abbildung des K-Vektorraumes V in den K^2-Vektorraum K. Daher ist $\mathrm{Rg}_K(V/H) \leq [K : K^2]$. Ist K perfekt, so ist $K = K^2$, so dass in diesem Falle $\mathrm{Rg}_K(V/H) = 1$ ist. Damit ist alles bewiesen.

Wir setzen $H_0 := H \cap H^\pi$. Ferner seien $H_1, H_2, H_3 \in \mathrm{L}(V)$ mit $H = H_0 \oplus H_1$, $H^\pi = H_0 \oplus H_2$ und $H_1^\pi \cap H_2^\pi = H_0 \oplus H_3$. Dann ist

$$H_0 \oplus H_1 \oplus H_2 = H + H^\pi$$

und somit

$$H_0^\pi \cap (H_1 + H_2)^\pi = H_0.$$

Wegen $H_0^\pi = H + H^\pi$ ist daher nach dem Modulargesetz

$$\begin{aligned} H_0 &= \big(H_0 + (H_1 + H_2)\big) \cap (H_1 + H_2)^\pi \\ &= H_0 + \big((H_1 + H_2) \cap (H_1 + H_2)^\pi\big) \end{aligned}$$

Also ist

$$(H_1 + H_2) \cap (H_1 + H_2)^\pi \leq H_0.$$

Hieraus folgt

$$(H_1 + H_2) \cap (H_1 + H_2)^\pi \leq H_0 \cap (H_1 + H_2) = \{0\},$$

so dass also

$$(H_1 + H_2) \cap (H_1 + H_2)^\pi = \{0\}$$

ist. Nach 1.5 ist daher

$$\begin{aligned} V &= H_1 \oplus H_2 \oplus (H_1 + H_2)^\pi \\ &= H_1 \oplus H_2 \oplus H_0 \oplus H_3 \\ &= (H + H^\pi) \oplus H_3. \end{aligned}$$

Es ist $H_0+H_2+H_3 \leq H_1^\pi$, so dass $V = H_1+H_1^\pi$ ist. Mit 1.5 erhalten wir daher $H_1 \cap H_1^\pi = \{0\}$. Folglich induziert f in H_1 eine nicht ausgeartete, alternierende Bilinearform. Mit $\mathrm{Sp}(H_1)$ bezeichnen wir die zu der von f in H_1 induzierten Form gehörige symplektische Gruppe.

4.2. Satz. *Es sei V ein Vektorraum des Ranges mindestens* 3 *über dem kommutativen Körper K der Charakteristik* 2. *Ferner sei π eine projektive Polarität von $\mathrm{L}(V)$, die nicht symplektisch sei. Ferner sei f eine π darstellende Bilinearform. Schließlich haben H, H_0, H_1, H_2 und H_3 die oben eingeführten Bedeutungen. Ist $\sigma \in C(\pi)$, so gibt es Abbildungen $\alpha \in \mathrm{Hom}_K(H_3, H_0)$, $\beta \in \mathrm{Hom}_K(H_3, H_1)$, $\gamma \in \mathrm{Sp}(H_1)$ und $\delta \in \mathrm{Hom}_K(H_1, H_0)$, so dass*
(j) *$f(y, z^\alpha) + f(y^\alpha, z) + f(y^\beta, z^\beta) = 0$ für alle y, $z \in H_3$ und*
(ij) *$f(x^\gamma, h^\beta) + f(x^\delta, h) = 0$ für alle $x \in H_1$ und alle $h \in H_3$ sowie*
(iij) *$(h_0 + h_1 + h_2 + h_3)^\sigma = h_0 + h_1^\gamma + h_1^\delta + h_2 + h_3 + h_3^\alpha + h_3^\beta$ für alle $h_i \in H_i$ gilt.*

Ist umgekehrt $\alpha \in \mathrm{Hom}_K(H_3, H_0)$, $\beta \in \mathrm{Hom}_K(H_3, H_1)$, $\gamma \in \mathrm{Sp}(H_1)$ und $\delta \in \mathrm{Hom}_K(H_1, H_0)$ und gelten (j) *und* (ij) *für diese Abbildungen, so liegt die durch* (iij) *erklärte Abbildung σ in $C(\pi)$. Die Zuordnung $\sigma \to (\alpha, \beta, \gamma, \delta)$ ist bijektiv.*

Beweis. Es sei $\sigma \in C(\pi)$. Dann ist offenbar $H^\sigma = H$ und damit auch $H^{\pi\sigma} = H^\pi$ und $H_0^\sigma = H_0$. Es sei $y \in H_2 + H_3$. Es gibt dann Homomorphismen $\eta \in \mathrm{Hom}_K(H_2{+}H_3, H_2{+}H_3)$ und $\zeta \in \mathrm{Hom}_K(H_2{+}H_3, H_0{+}H_1)$ mit $y^\sigma = y^\eta{+}y^\zeta$. Daher ist

$$f(y, y) = f(y^\sigma, y^\sigma) = f(y^\eta, y^\eta) + (f(y^\zeta, y^\zeta).$$

Weil $H_0 + H_1 = H$ ist, ist $f(y^\zeta, y^\zeta) = 0$. Somit ist $f(y, y) = f(y^\eta, y^\eta)$, was wiederum $f(y^\eta + y, y^\eta + y) = 0$ nach sich zieht. Daher ist

$$y^\eta + y \in H \cap (H_2 + H_3) = \{0\},$$

so dass für alle $y \in H_2 + H_3$ die Gleichung $y^\eta = y$ gilt.

Es sei $y \in H_2$. Nach dem soeben Bewiesenen ist dann $y^\sigma = y + y^\zeta$ mit $y^\zeta \in H$. Wegen $H_2 \leq H^\pi = H^{\pi\sigma}$ ist daher

$$y^\zeta = y^\sigma + y \in (H_2^\sigma + H_2) \cap H \leq H^\pi \cap H = H_0.$$

Mit $u \in H_3$ folgt somit

$$\begin{aligned} f(u, y) &= f(u^\sigma, y^\sigma) = f(u + u^\zeta, y + y^\zeta) \\ &= f(u, y) + f(u, y^\zeta) + f(u^\zeta, y) + f(u^\zeta, y^\zeta). \end{aligned}$$

Nun ist $u^\zeta \in H$ und $y \in H_2 \leq H^\pi$, so dass $f(u^\zeta, y) = 0$ ist. Ebenso folgt $f(u^\zeta, y^\zeta) = 0$. Folglich ist

$$f(u, y) = f(u, y) + f(u, y^\zeta),$$

so dass auch $f(u, y^\zeta) = 0$ ist für alle $u \in H_3$ und alle $y \in H_2$. Hieraus folgt

$$y^\zeta \in H_3^\pi \cap H_0 = H_3^\pi \cap H \cap H^\pi = (H_3 + H + H^\pi)^\pi = V^\pi = \{0\}$$

für alle $y \in H_3$. Somit ist $y^\sigma = y$ für alle $y \in H_2$.

Es sei $y \in H_0$ und $x \in H_3$. Dann ist

$$f(y,x) = f(y^\sigma, x^\sigma) = f(y^\sigma, x + x^\zeta) = f(y^\sigma, x) + f(y^\sigma, x^\zeta).$$

Nun ist $y^\sigma \in H_0^\sigma = H_0$ und $x^\zeta \in H$, so dass $f(y^\sigma, x^\zeta) = 0$ ist. Hieraus folgt

$$f(y - y^\sigma, x) = 0$$

für alle $y \in H_0$ und alle $x \in H_3$. Folglich ist

$$y - y^\sigma \in H_3^\pi \cap H_0 = \{0\}.$$

Also induziert σ auch in H_0 die Identität. Wegen $H^\pi = H_0 + H_2$ ist $y^\sigma = y$ für alle $y \in H^\pi$.

Bevor wir den Beweis zu Ende führen, machen wir noch die folgende Bemerkung: ist $H = \{0\}$, so ist $H^\pi = V$ und daher $C(\pi) = \{1\}$. Dieser Fall kann durchaus eintreten. Ist nämlich K nicht perfekt und ist $[K : K^2] = n \geq 3$, ist ferner $k_1, \ldots, k_n$ eine Basis von K bez. K^2 und V ein Vektorraum über K mit $3 \leq \mathrm{Rg}_K(V) = m < n$, ist schließlich $b_1, \ldots, b_m$ eine Basis von V über K und definiert man f vermöge

$$f\left(\sum_{i:=1}^m b_i x_i, \sum_{i:=1}^m b_i y_i\right) := \sum_{i:=1}^m k_i x_i y_i,$$

so ist f eine nicht entartete Bilinearform auf V, für die genau dann $f(x,x) = 0$ gilt, wenn $x = 0$ ist.

Es sei $x \in H_3$. Dann ist $x^\zeta \in H = H_0 \oplus H_1$. Es gibt daher ein $\alpha \in \mathrm{Hom}_K(H_3, H_0)$ und ein $\beta \in \mathrm{Hom}_K(H_3, H_1)$ mit $x^\zeta = x^\alpha + x^\beta$.

Es sei $x \in H_1$. Dann ist $x^\sigma = x^\gamma + x^\delta$ mit $\gamma \in \mathrm{Hom}_K(H_1, H_1)$ und $\delta \in \mathrm{Hom}_K(H_1, H_0)$, da ja

$$x^\sigma \in H_1^\sigma \leq H^\sigma = H = H_0 \oplus H_1$$

ist. Sind x, $y \in H_1$, so ist also

$$f(x,y) = f(x^\sigma, y^\sigma) = f(x^\gamma + x^\delta, y^\gamma + y^\delta) = f(x^\gamma, y^\gamma).$$

Ist $x^\gamma = 0$, so ist $f(x,y) = 0$ für alle $y \in H_1$. Weil f, wie wir gesehen haben, in H_1 eine nicht ausgeartete, alternierende Bilinearform induziert, folgt weiter, dass $x = 0$ ist. Folglich ist γ injektiv und wegen der Endlichkeit von $\mathrm{Rg}_K(H_1)$ dann auch bijektiv. Hieraus und aus $f(x^\gamma, y^\gamma) = f(x,y)$ für alle x, $y \in H_1$ folgt schließlich $\gamma \in \mathrm{Sp}(H_1)$.

Ist nun $h_i \in H_i$ für $i := 0, 1, 2, 3$, so ist also

$$\begin{aligned}(h_0 + h_1 + h_2 + h_3)^\sigma &= h_0^\sigma + h_1^\sigma + h_2^\sigma + h_3^\sigma \\ &= h_0 + h_1^\gamma + h_1^\delta + h_2 + h_3^\alpha + h_3^\beta.\end{aligned}$$

Damit ist (iij) nachgewiesen. Um (j) zu beweisen, seien y, $z \in H_3$. Dann ist

$$\begin{aligned} f(y,z) = f(y^\sigma, z^\sigma) &= f(y + y^\alpha + y^\beta, z + z^\alpha + z^\beta) \\ &= f(y,z) + f(y,z^\alpha) + f(y,z^\beta) + f(y^\alpha,z) + f(y^\alpha,z^\alpha) \\ &\quad + f(y^\alpha,z^\beta) + f(y^\beta,z) + f(y^\beta,z^\alpha) + f(y^\beta,z^\beta). \end{aligned}$$

Wegen $H_3 \le H_1^\pi$ ist

$$f(y,z^\beta) = 0 = f(y^\beta, z).$$

Ferner ist $H_0 \le H_0^\pi$, H_1^π, so dass auch

$$f(y^\alpha, z^\alpha) = 0 = f(y^\alpha, z^\beta) = f(y^\beta, z^\alpha)$$

ist. Aus obiger Gleichung für $f(y,z)$ folgt somit

$$f(y,z^\alpha) + f(y^\alpha,z) + f(y^\beta,z^\beta) = 0,$$

dh. (j).

Schließlich sei $x \in H_1$ und $h \in H_3$. Wegen $H_3 \le H_1^\pi$ ist dann $f(x,h) = 0 = f(x^\gamma, h)$. Daher ist

$$\begin{aligned} 0 = f(x,h) &= f(x^\sigma, h^\sigma) = f(x^\gamma + x^\delta, h + h^\alpha + h^\beta) \\ &= f(x^\gamma,h) + f(x^\gamma,h^\alpha) + f(x^\gamma,h^\beta) + f(x^\delta,h) + f(x^\delta,h^\alpha) + f(x^\delta,h^\beta). \end{aligned}$$

Wegen $h^\alpha \in H_0$ ist $f(x^\gamma, h^\alpha) = 0 = f(x^\delta, h^\alpha)$. Ferner ist $x^\delta \in H_0$ und $h^\beta \in H_1$, so dass auch $f(x^\delta, h^\beta) = 0$ ist. Daher gilt

$$0 = f(x^\gamma, h^\beta) + f(x^\delta, h),$$

dh. (ij).

Es bleibe dem Leser überlassen zu verifizieren, dass umgekehrt jedes Quadrupel $(\alpha,\beta,\gamma,\delta)$, welches (j) und (ij) erfüllt, vermöge (iij) ein $\sigma \in C(\pi)$ liefert und dass die Zuordnung $\sigma \to (\alpha,\beta,\gamma,\delta)$ injektiv ist.

4.3. Satz. *Es sei V ein Vektorraum des Ranges mindestens* 3 *über dem kommutativen Körper K der Charakteristik* 2. *Ferner sei π eine projektive Polarität von* $\mathrm{L}(V)$*, die nicht symplektisch sei. Ferner seien ρ, $\sigma \in C(\pi)$. Gehört zu ρ gemäß 4.2 das Quadrupel $(\alpha,\beta,\gamma,\delta)$ und zu σ das Quadrupel $(\alpha',\beta',\gamma',\delta')$, so gehört zu $\rho\sigma$ das Quadrupel*

$$(\alpha + \alpha' + \beta\delta', \beta' + \beta\gamma', \gamma\gamma', \gamma\delta' + \delta).$$

Beweis. Es sei $(\alpha'',\beta'',\gamma'',\delta'')$ das zu $\rho\sigma$ gehörende Quadrupel. Ist $h_1 \in H_1$, so ist $h_1^\rho = h_1^\gamma + h_1^\delta$. Daher ist

$$h_1^{\rho\sigma} = h_1^{\gamma\sigma} + h_1^{\delta\sigma} = h_1^{\gamma\gamma'} + h_1^{\gamma\delta'} + h_1^\delta.$$

Somit ist $\gamma'' = \gamma\gamma'$ und $\delta'' = \gamma\delta' + \delta$. Ist $h_3 \in H_3$, so ist

$$h_3^{\rho\sigma} = h_3^\sigma + h_3^{\alpha\sigma} + h_3^{\beta\sigma} = h_3 + h_3^{\alpha'} + h_3^{\beta'} + h_3^\alpha + h_3^{\beta\gamma'} + h_3^{\beta\delta'}.$$

Also ist $\alpha'' = \alpha + \alpha' + \beta\delta'$ und $\beta'' = \beta' + \beta\gamma'$. Damit ist alles bewiesen.

4.4. Satz. *Es sei V ein Vektorraum des Ranges mindestens 3 über dem kommutativen Körper K der Charakteristik 2. Ferner sei π eine projektive Polarität von $\mathrm{L}(V)$, die nicht symplektisch sei. Ferner sei $\rho \in C(\pi)$ und zu ρ gehöre gemäß 4.2 das Quadrupel $(\alpha, \beta, \gamma, \delta)$. Genau dann liegt ρ im Zentrum von $C(\pi)$, wenn $\beta = 0$, $\gamma = 1$ und $\delta = 0$ ist.*

Beweis. Es sei $\sigma \in C(\pi)$ und $(\alpha', \beta', \gamma', \delta')$ sei das zugehörige Quadrupel. Nach 4.3 ist genau dann $\rho\sigma = \sigma\rho$, wenn

$$\begin{aligned} \alpha + \alpha' + \beta\delta' &= \alpha' + \alpha + \beta'\delta, \\ \beta' + \beta\gamma' &= \beta + \beta'\gamma, \\ \gamma\gamma' &= \gamma'\gamma, \\ \gamma\delta' + \delta &= \gamma'\delta + \delta' \end{aligned}$$

ist. Nach 4.3 entspricht jedem Quadrupel der Form $(0, 0, \gamma', 0)$ ein $\sigma \in C(\pi)$. Ist nun $\rho \in Z(C(\pi))$, so ist also $\beta\gamma' = \beta$, $\gamma\gamma' = \gamma'\gamma$ und $\delta = \gamma'\delta$ für alle $\gamma' \in \mathrm{Sp}(H_1)$. Hieraus folgt $\beta = 0$ und $\delta = 0$ sowie $\gamma \in Z(\mathrm{Sp}(\pi))$. Weil die Charakteristik von K gleich 2 ist, ist $Z(\mathrm{Sp}(H_1)) = \{1\}$, so dass $\gamma = 1$ ist.

Ist umgekehrt $(\alpha, \beta, \gamma, \delta) = (\alpha, 0, 1, 0)$, so ist $\rho \in Z(\mathrm{Sp}(\pi))$.

4.5. Satz. *Es sei V ein Vektorraum des Ranges mindestens 3 über dem kommutativen Körper K der Charakteristik 2. Ferner sei π eine projektive Polarität von $\mathrm{L}(V)$, die nicht symplektisch sei. Dann enthält $C(\pi)$ einen Normalteiler M mit $Z(C(\pi)) \subseteq M \subseteq C(\pi)$ mit $\mathrm{Sp}(H_1) \cong C(\pi)/M$ und $M' \subseteq Z(C(\pi))$.*

Beweis. Es sei M die Menge aller $\rho \in C(\pi)$, für die das zugehörige Quadrupel die Form $(\alpha, \beta, 1, \delta)$ hat. Aus 4.3 folgt, dass M ein Normalteiler von $C(\pi)$ ist. Ist ferner G die Menge aller $\rho \in C(\pi)$, deren zugehöriges Quadrupel die Form $(0, 0, \gamma, 0)$ hat, so ist G eine zu $\mathrm{Sp}(H_1)$ isomorphe Untergruppe von $C(\pi)$ mit $C(\pi) = GM$ und $G \cap M = \{1\}$. Also ist $C(\pi)/M$ zu $\mathrm{Sp}(H_1)$ isomorph. Aus 4.4 folgt $Z(C(\pi)) \subseteq M$ und mit 4.3 folgt schließlich $M' \subseteq Z(C(\pi))$.

4.6. Satz. *Die Voraussetzungen seien wie in 4.5. Ist K perfekt, so gilt:*
a) *Ist $\mathrm{Rg}_K(V) = n$ ungerade, so ist $M = \{1\}$ und $C(\pi) \cong \mathrm{Sp}(n-1, K)$.*
b) *Ist $\mathrm{Rg}_K(V) = n$ gerade, so ist $Z(C(\pi))$ zur additiven Gruppe von K und $M/Z(C(\pi))$ zu $\mathrm{Hom}_K(H_3, H_1)$ isomorph.*

Beweis. Weil K perfekt ist, ist H nach 4.1 eine Hyperebene. Folglich ist H^π ein Punkt. Wegen $H_0 \leq H^\pi$ folgt daher, dass $\mathrm{Rg}_K(H_0) \leq 1$ ist. Ferner ist $\mathrm{Rg}_K(H_1)$ gerade.

a) Ist $\mathrm{Rg}_K(V)$ ungerade, so ist $\mathrm{Rg}_K(H)$ gerade. Wegen

$$\mathrm{Rg}_K(H) = \mathrm{Rg}_K(H_0) + \mathrm{Rg}_K(H_1)$$

ist daher auch $\mathrm{Rg}_K(H_0)$ gerade, so dass $\mathrm{Rg}_K(H_0) = 0$ und damit $H_0 = \{0\}$ ist. Also ist $H = H_1$ und $H^\pi = H_2$. Hieraus folgt mit

$$H_3 \oplus H_0 = H_1^\pi \cap H_2^\pi = H^\pi \cap H = H_0 = \{0\},$$

dass auch $H_3 = \{0\}$ ist. Daher ist $\mathrm{Hom}_K(H_3, H_0) = \{0\}$ und $\mathrm{Hom}_K(H_3, H_1) = \{0\}$. Wegen $H_0 = \{0\}$ ist auch $\mathrm{Hom}_K(H_1, H_0) = \{0\}$. Dies impliziert wiederum $M = \{1\}$. Wegen $H_1 = H$ ist daher

$$C(\pi) \cong \mathrm{Sp}(H_1) \cong \mathrm{Sp}(n-1, K).$$

b) Ist $\mathrm{Rg}_K(V)$ gerade, so ist $\mathrm{Rg}_K(H)$ ungerade. Wegen

$$\mathrm{Rg}_K(H_0) = \mathrm{Rg}_K(H) - \mathrm{Rg}_K(H_1)$$

ist dann auch $\mathrm{Rg}_K(H_0)$ ungerade. Weil der Rang von H_0 höchstens Eins ist, ist also $\mathrm{Rg}_K(H_0) = 1$. Insbesondere ist dann $\mathrm{Rg}_K(H_1) = n-2$, was seinerseits $\mathrm{Rg}(H_1^\pi) = 2$ impliziert. Weil $\mathrm{Rg}_K(H_0) = 1 = \mathrm{Rg}_K(H^\pi)$ ist, ist $H^\pi = H_0$, so dass $H_2 = \{0\}$ ist. Dies besagt wiederum $H_2^\pi = V$. Also ist

$$H_1^\pi = H_1^\pi \cap H_2^\pi = H_0 \oplus H_3,$$

so dass

$$\mathrm{Rg}_K(H_3) = \mathrm{Rg}_K(H_1^\pi) - \mathrm{Rg}_K(H_0) = 2 - 1 = 1$$

ist. Wegen

$$V = H_0 \oplus H_1 \oplus H_3 = H_1 \oplus H_1^\pi$$

ist H_1^π nicht isotrop. Es gibt daher Vektoren p und q mit $H_0 = pK$ und $H_3 = qK$ und $f(p,q) = 1$. Es sei nun $\alpha \in \mathrm{Hom}_K(H_3, H_0)$ und $\beta \in \mathrm{Hom}_K(H_3, H_1)$. Sind $y,\ z \in H_3$, so sind y und z linear abhängig. Dann sind aber auch y^β und z^β linear abhängig, so dass $f(y^\beta, z^\beta) = 0$ ist. Es sei $q^\alpha = pr$ und $y = qs$ sowie $z = qt$. Dann ist

$$f(y, z^\alpha) + f(y^\alpha, z) + f(y^\beta, z^\beta) = f(q,p)srt + f(p,q)srt = 0,$$

so dass die Bedingung (j) von 4.2 stets erfüllt ist.

Es sei $h = qr \in H_3$. Genau dann ist

$$0 = f(x\gamma, q^\beta)r + f(x\delta, q)r$$

für alle $r \in K$, wenn

$$0 = f(x^\gamma, q^\beta) + f(x^\delta, q)$$

ist. Definiert man nun φ durch $x^\delta = p\varphi(x)$, so ist $\varphi \in \mathrm{Hom}_K(H_1, K)$ und es gilt

$$0 = f(x^\gamma, q^\beta) + f(p,q)\varphi(x) = f(x^\gamma, q^\beta) + \varphi(x),$$

so dass $\varphi(x) = f(x^\gamma, q^\beta)$ ist. Dies zeigt, dass

$$x^\delta = pf(x^\gamma, q^\beta)$$

ist.

Sind umgekehrt α, β, γ gegeben und definiert man δ durch

$$x^\delta := pf(x^\gamma, q^\beta),$$

so erfüllt das Quadrupel $(\alpha, \beta, \gamma, \delta)$ die Bedingung (j) sowieso und auch die Bedingung (ij), wie man leicht nachrechnet. Hieraus folgt alles Weitere.

5. Quadratische Formen

Es sei V ein Vektorraum endlichen Ranges über dem kommutativen Körper K. Eine Abbildung Q von V in K nennen wir, wie schon in Kapitel IIII, Abschnitt 4, *quadratische Form* auf V, falls Q die beiden folgenden Bedingungen erfüllt:
1) Es ist $Q(xk) = Q(x)k^2$ für alle $x \in V$ und alle $k \in K$.
2) Die durch $f(x,y) := Q(x+y) - Q(x) - Q(y)$ erklärte Abbildung f von $V \times V$ in K ist eine Bilinearform.

Es ist
$$f(x,x) = Q(2x) - 2Q(x) = 4Q(x) - 2Q(x) = 2Q(x),$$
so dass f alternierend ist, falls $\mathrm{Char}(K) = 2$ ist. Ferner ist klar, dass $f(x,y) = f(y,x)$ ist, so dass f also in jedem Fall symmetrisch ist. Man nennt f die zu Q *assoziierte Bilinearform*. Ist $\mathrm{Char}(K) \neq 2$, so ist $Q(x) = \frac{1}{2}f(x,x)$. Die quadratische Form Q heißt *nicht ausgeartet*, falls die zu Q assoziierte Bilinearform f nicht ausgeartet ist. Ist $\mathrm{Char}(K) = 2$, so ist f alternierend, so dass Q höchstens dann nicht ausgeartet ist, wenn $\mathrm{Rg}_K(V)$ gerade ist.

Ist Q eine quadratische Form auf V und ist f die zu Q assoziierte Bilinearform, so heißt die Menge
$$\mathrm{Kern}(Q) := \{x \mid x \in V, Q(x) = 0 \text{ und } f(x,y) = 0 \text{ für alle } y \in V\}$$
Kern von Q. Offenbar ist $\mathrm{Kern}(Q)$ ein Unterraum von V. Ist nämlich $x \in \mathrm{Kern}(Q)$ und $k \in K$, so ist
$$Q(xk) = Q(x)k^2 = 0$$
und
$$f(xk,y) = f(x,y)k = 0$$
für alle $y \in V$. Also ist $xk \in \mathrm{Kern}(Q)$. Sind x, $x' \in \mathrm{Kern}(Q)$, so ist
$$Q(x+x') = f(x,x') + Q(x) + Q(x') = 0$$
und
$$f(x+x',y) = f(x,y) + f(x',y) = 0$$
für alle $y \in V$. Daher ist auch $x + x' \in \mathrm{Kern}(Q)$.

Die quadratische Form Q heißt *singulär*, falls $\mathrm{Kern}(Q) \neq \{0\}$ ist.

5.1. Satz. *Es sei V ein Vektorraum endlichen Ranges über dem kommutativen Körper K und Q sei eine quadratische Form auf V.*
a) *Ist Q singulär, so ist Q ausgeartet.*
b) *Ist $\mathrm{Char}(K) \neq 2$ und ist Q ausgeartet, so ist Q singulär.*

Beweis. a) Es sei Q singulär. Es gibt dann einen von 0 verschiedenen Vektor $x \in \mathrm{Kern}(Q)$. Für diesen Vektor gilt $f(x,y) = 0$ für alle $y \in V$, so dass Q ausgeartet ist.

b) Q sei ausgeartet. Es gibt dann einen Vektor $x \in V$ mit $x \neq 0$ und $f(x,y) = 0$ für alle $y \in V$. Insbesondere ist dann auch
$$0 = f(x,x) = 2Q(x).$$

Weil $\mathrm{Char}(K) \neq 2$ ist, folgt $Q(x) = 0$, so dass $x \in \mathrm{Kern}(Q)$ ist. Folglich ist Q singulär.

Dass es im Falle der Charakteristik 2 ausgeartete quadratische Formen gibt, die nicht singulär sind, zeigt folgendes Beispiel. Es sei K ein Körper der Charakteristik 2 und V sei ein Vektorraum des Ranges 3 über K und b_1, b_2, b_3 sei eine Basis von V. Ist $v = b_1k_1 + b_2k_2 + b_3k_3$, so setzen wir

$$Q(v) := k_1^2 + k_2k_3 + k_3^2.$$

Ist dann auch noch $w = b_1l_1 + b_2l_2 + b_3l_3$, so ist — hier wird benutzt, dass $\mathrm{Char}(K) = 2$ ist —,

$$f(v, w) = l_2k_3 + k_2l_3.$$

Hieraus folgt, dass $f(v, w) = 0$ für alle $w \in V$ genau dann gilt, wenn $v \in b_1K$ ist. Also ist $\mathrm{Kern}(Q) \leq b_1K$. Nun ist $Q(b_1) = 1$, so dass $\mathrm{Kern}(Q) = \{0\}$ ist.

Ist Q eine quadratische Form auf dem Vektorraum V und ist f die zu Q assoziierte Bilinearform, so definieren wir das *Radikal* $\mathrm{rad}(Q)$ von Q durch

$$\mathrm{rad}(Q) := \big\{x \mid x \in V, f(x, y) = 0 \text{ für alle } y \in V\big\}.$$

Offenbar ist $\mathrm{rad}(Q)$ ein Unterraum.

5.2. Satz. *Es sei K ein perfekter Körper der Charakteristik 2. Ferner sei V ein Vektorraum über K und Q sei eine quadratische Form auf V. Dann ist Q sicher dann singulär, wenn $\mathrm{Rg}_K(\mathrm{rad}(Q)) \geq 2$ ist.*

Beweis. Es seien a und b zwei linear unabhängige Vektoren aus $\mathrm{rad}(Q)$. Ist $Q(a) = 0$ oder $Q(b) = 0$, so ist Q singulär. Wir können daher annehmen, dass $Q(a)$, $Q(b) \neq 0$ ist. Es gibt dann, da K perfekt ist, ein $k \in K$ mit

$$k^2 = \frac{Q(a)}{Q(b)}.$$

Weil a und b linear unabhängig sind, ist $a + bk \neq 0$. Ferner ist $a + bk \in \mathrm{rad}(Q)$, da $\mathrm{rad}(Q)$ ja ein Unterraum von V ist. Schließlich gilt

$$Q(a + bk) = f(a, b)k + Q(a) + Q(b)k^2 = 0,$$

so dass $0 \neq a + bk \in \mathrm{Kern}(Q)$ ist, q. e. d.

5.3. Satz. *Es sei K ein perfekter Körper der Charakteristik 2 und V sei ein Vektorraum geraden Ranges über K. Ist Q eine quadratische Form auf V, so ist Q genau dann nicht singulär, wenn Q nicht entartet ist.*

Beweis. Ist Q nicht entartet, so ist Q nach 5.1 a) nicht singulär.

Ist Q entartet, so ist $\mathrm{rad}(Q) \neq \{0\}$. Weil die zu Q assoziierte Bilinearform f alternierend ist, induziert f in $V/\mathrm{rad}(Q)$ eine alternierende Bilinearform, die überdies nicht ausgeartet ist. Nach 1.6 ist somit $\mathrm{Rg}_K(V/\mathrm{rad}(Q))$ gerade. Weil $\mathrm{Rg}_K(V)$ gerade ist, ist auch $\mathrm{Rg}_K(\mathrm{rad}(Q))$ gerade. Wegen $\mathrm{rad}(Q) \neq \{0\}$ ist somit $\mathrm{Rg}_K(\mathrm{rad}(Q)) \geq 2$, so dass Q nach 5.2 singulär ist. Damit ist alles bewiesen.

Es sei Q eine quadratische Form auf V und U sei der Kern von Q. Ist $v \in V$ und $u \in U$, so ist

$$Q(v+u) = f(v,u) + Q(v) + Q(u) = Q(v).$$

Definiert man Q' auf V/U durch $Q'(v+U) := Q(v)$, so ist also Q' eine Abbildung von V/U in K. Ferner ist

$$Q'(vk+U) = Q(vk) = Q(v)k^2 = Q'(v+U)k^2.$$

Definiert man f' durch

$$f'(v+U, w+U) := Q'(v+w+U) - Q'(v+U) - Q'(w+U),$$

so folgt

$$f'(v+U, w+U) = f(v,w).$$

Dies impliziert, dass auch f' eine Bilinearform ist. Folglich ist Q' eine quadratische Form auf V/U. Ist $f'(v+U, w+U) = 0$ für alle $w+U \in V/U$ und ist $Q'(v+U) = 0$, so ist $f(v,w) = 0$ für alle $w \in V$ und $Q(v) = 0$. Also ist $v \in U$. Somit ist Q' nicht singulär. Hieraus folgt, dass man eine Übersicht über alle quadratischen Formen hat, wenn man alle nicht singulären quadratischen Formen kennt.

Ein Vektor $v \in V$ heißt *singulär*, falls $v \neq 0$ und $Q(v) = 0$ ist. Ist v singulär, so ist vk singulär für alle $k \in K^*$. Ferner ist $f(w,w') = 0$ für alle w, $w' \in vK$. Ist $U \in \mathrm{L}(V)$ und ist $Q(u) = 0$ und $f(u,w) = 0$ für alle u, $w \in U$, so heißt U *vollständig singulär*. Die von singulären Vektoren aufgespannten Punkte sind also vollständig singulär.

Die Menge der zu Q gehörenden vollständig singulären Punkte nennen wir die zu Q *gehörende*, bzw. die *durch Q definierte Quadrik*. Ist Q nicht singulär, so nennen wir die zugehörige Quadrik, auch wenn sie leer sein sollte, *nicht ausgeartet*. Ist Q singulär, so nennen wir die zugehörige Quadrik, die dann niemals leer ist, auch *Kegel*. Ist U der Kern von Q, so ist der durch Q definierte Kegel offensichtlich die Projektion der zu Q' gehörenden Quadrik in $\mathrm{L}(V/U)$ aus U. Dies rechtfertigt den Namen Kegel.

Sind Σ und Σ' Quadriken in $\mathrm{L}(V)$, so heißen Σ und Σ' *projektiv äquivalent*, falls es eine projektive Kollineation von $\mathrm{L}(V)$ gibt, welche Σ auf Σ' abbildet. Sind Q und Q' quadratische Formen, so heißen sie *projektiv äquivalent*, falls es ein $k \in K^*$ und ein $\sigma \in \mathrm{GL}(V)$ gibt mit $Q(x) = kQ'(x^\sigma)$ für alle $x \in V$. Sind Σ und Σ' projektiv äquivalente Quadriken und wird Σ durch die quadratische Form Q dargestellt, so definieren wir die quadratische Form Q' durch $Q'(x) := Q(x^{\gamma^{-1}})$ für alle $x \in V$, wobei $\gamma \in \mathrm{GL}(V)$ so gewählt sei, dass $\Sigma^\gamma = \Sigma'$ ist. Nun ist genau dann $Q'(x) = 0$, wenn $Q(x^{\sigma^{-1}}) = 0$ ist. Hieraus folgt, dass Σ' durch Q' dargestellt wird. Damit ist gezeigt, dass projektiv äquivalente Quadriken durch projektiv äquivalente quadratische Formen dargestellt werden. Die Umkehrung, dass projektiv äquivalente quadratische Formen projektive äquivalente Quadriken darstellen ist ebenso einfach zu zeigen.

5.4. Satz. *Es sei Q eine quadratische Form auf dem Vektorraum V. Ist U ein Teilraum von V, dessen Punkte alle auf der durch Q definierten Quadrik liegt, so ist U vollständig singulär.*

Beweis. Es seien x, $y \in U$. Dann ist $Q(x) = Q(y) = Q(x + y) = 0$. Daher ist

$$f(x, y) = Q(x + y) - Q(x) - Q(y) = 0.$$

Damit ist bereits alles bewiesen.

6. Die wittsche Zerlegung

Es sei f eine symmetrische α-Semibilinearform auf V. Die Form f heißt *spurwertig*, falls es zu jedem $x \in V$ ein $k \in K$ gibt mit $f(x, x) = k + k^\alpha$.

Ist die Charakteristik von K ungerade, so gilt wegen $f(x, x)^\alpha = f(x, x)$ die Gleichung

$$f(x, x) = \frac{1}{2} f(x, x) + \left(\frac{1}{2} f(x, x)\right)^\alpha,$$

so dass f spurwertig ist.

Ist f alternierend, so ist $f(x, x) = 0 + 0^\alpha$, so dass f auch in diesem Falle spurwertig ist.

Ist $\mathrm{Char}(K) = 2$ und induziert α auf $Z(K)$ nicht die Identität, so gibt es nach III.6.3b) ein $z \in Z(K)$ mit $z + z^\alpha = 1$. Dann ist

$$f(x, x) = f(x, x)(z + z^\alpha) = f(x, x)z + (f(x, x)z)^\alpha,$$

so dass f auch in diesem Falle spurwertig ist. Dieser Fall liegt insbesondere dann vor, wenn K kommutativ und α ein involutorischer Automorphismus von K ist.

Ist f die zu einer quadratischen Form assoziierte Bilinearform, so ist f ebenfalls spurwertig. Dies ist für $\mathrm{Char}(K) \neq 2$ nach obigem selbstverständlich und folgt für $\mathrm{Char}(K) = 2$ daraus, dass f in diesem Falle alternierend ist.

Dass es auch nicht spurwertige symmetrische Bilinearformen gibt, zeigen die Beispiele von projektiven Polaritäten, die wir in Abschnitt 4 betrachtet haben.

Wir setzen im Folgenden stets voraus, dass f eine spurwertige, symmetrische α-Semibilinearform auf V ist, wobei wir statt α-Semibilinearform auch kurz α-Form sagen werden. Nach obiger Bemerkung kann f also auch die zu einer quadratischen Form assoziierte Bilinearform sein. Sind x und y zwei Vektoren aus V und ist $f(x, y) = 0$, so nennen wir x und y *orthogonal*. Ist $U \in \mathrm{L}(V)$, so bezeichnen wir mit $U^\perp$ die Menge aller zu allen Vektoren aus U orthogonalen Vektoren. Zwei Unterräume U und W heißen *orthogonal*, falls $W \leq U^\perp$ ist. Weil f symmetrisch ist, ist auch die Orthogonalitätsrelation symmetrisch.

Ist $U \cap U^\perp \neq \{0\}$, so heißt U, wie schon zuvor, *isotrop*. Rührt f von einer quadratischen Form Q her, so heißt U *singulär*, falls U isotrop ist und außerdem $Q(u) = 0$ ist für alle $u \in U \cap U^\perp$. Wir nennen U *vollständig singulär*, falls U vollständig isotrop und singulär ist. Diesen Begriff hatten wir schon früher definiert. Man beachte, dass nicht isotrope Räume nicht singulär sind.

6.1. Satz. *Es sei V ein Vektorraum über K und f sei entweder eine spurwertige α-Form oder die zu der quadratischen Form Q auf V assoziierte Bilinearform. Ferner sei U ein von $\{0\}$ verschiedener, vollständig isotroper, bzw. vollständig singulärer Unterraum von V. Ist $x \in V$ und $x \notin U^\perp$, ist ferner $k \in K$, so gibt es ein $y \in U$ mit $f(x+y, x+y) = k + k^\alpha$, bzw. mit $Q(x+y) = k$.*

Beweis. Wir betrachten zuerst den Fall, dass f eine α-Form ist. Da f spurwertig ist, gibt es ein $l \in K$ mit $f(x,x) = l + l^\alpha$. Ist $y \in U$, so ist $f(y,y) = 0$, da ja $U \leq U^\perp$ ist. Daher ist

$$\begin{aligned} f(x+y, x+y) &= f(x,x) + f(x,y) + f(y,x) + f(y,y) \\ &= l + l^\alpha + f(x,y) + f(x,y)^\alpha \\ &= l + f(x,y) + (l + f(x,y))^\alpha. \end{aligned}$$

Wegen $x \notin U^\perp$ ist die Abbildung $y \to f(x,y)$ eine von Null verschiedene lineare Abbildung von U in und damit auf K. Es gibt also ein $y \in U$ mit $f(x,y) = k - l$, womit der Satz im vorliegenden Falle bewiesen ist.

Es sei nun f die zu der quadratischen Form Q assoziierte Bilinearform. Wir setzen $l := Q(x)$. Ist $y \in U$, so ist $Q(y) = 0$, da U ja vollständig singulär ist. Es folgt also, dass

$$Q(x+y) = Q(x) + Q(y) + f(x,y) = l + f(x,y)$$

ist. Es ist wieder $f(x,y) \neq 0$, so dass wir wie im ersten Fall die Existenz eines $y \in U$ erschließen, welches $f(x,y) = k - l$ erfüllt. Dann ist $Q(x+y) = k$, so dass die Behauptung auch im zweiten Falle bewiesen ist.

6.2. Satz. *Es sei f eine spurwertige, nicht entartete, symmetrische α-Form auf dem K-Vektorraum V, bzw. die zu einer nicht entarteten quadratischen Form Q assoziierte Bilinearform. Ferner sei X ein vollständig isotroper, bzw. vollständig singulärer Unterraum von V.*

a) *Ist $Y \in \mathrm{L}(V)$ ein vollständig isotroper, bzw. vollständig singulärer Unterraum mit $\mathrm{Rg}_K(Y) = \mathrm{Rg}_K(X) = r$ und $Y \cap X^\perp = \{0\}$, so ist $X + Y$ nicht isotrop und zu jeder Basis $b_1, \ldots, b_r$ von X gibt es eine Basis $c_1, \ldots, c_r$ von Y mit $f(b_i, c_j) = \delta_{ij}$ für $i, j := 1, \ldots, r$.*

b) *Ist U ein vollständig isotroper bzw. vollständig singulärer Unterraum mit $\mathrm{Rg}_K(U) \leq \mathrm{Rg}_K(X)$ und $U \cap X^\perp = \{0\}$, so gibt es einen vollständig isotropen bzw. einen vollständig singulären Unterraum Y mit $U \leq Y$, $\mathrm{Rg}_K(Y) = \mathrm{Rg}_K(X)$ und $Y \cap X^\perp = \{0\}$.*

Beweis. a) Weil f nicht entartet ist, ist die Abbildung $\perp$ eine Polarität von $\mathrm{L}(V)$. Daher ist

$$(X+Y) \cap (X+Y)^\perp = (X+Y) \cap X^\perp \cap Y^\perp.$$

Wegen $X \leq X^\perp$ gilt daher auf Grund des Modulargesetzes, und weil $X \cap Y^\perp = \{0\}$ vorausgesetzt ist,

$$(X+Y) \cap X^\perp \cap Y^\perp = \bigl(X + (Y \cap X^\perp)\bigr) \cap Y^\perp = X \cap Y^\perp.$$

Nun ist $X^\perp \cap Y = \{0\}$ und daher $X + Y^\perp = V$. Weil f nicht entartet ist, ist $\mathrm{Rg}_K(Y) + \mathrm{Rg}_K(Y^\perp) = \mathrm{Rg}_K(V)$ und wegen $\mathrm{Rg}_K(X) = \mathrm{Rg}_K(Y)$ ist $\mathrm{Rg}_K(X) + \mathrm{Rg}_K(Y^\perp) = \mathrm{Rg}_K(V)$. Hieraus folgt, dass $V = X \oplus Y^\perp$ ist. Dies besagt wiederum $X \cap Y^\perp = \{0\}$. Also ist $(X+Y) \cap (X+Y)^\perp = \{0\}$, so dass $X + Y$ nicht isotrop, bzw. nicht singulär ist.

Wir definieren für $i := 1, \ldots, r$ die Abbildung $\varphi_i \in \mathrm{Hom}_K(Y, K)$ durch

$$\varphi_i(y) := f(b_i, y)$$

für alle $y \in Y$. Ferner setzen wir $H_i := \mathrm{Kern}(\varphi_i)$. Dann ist

$$\bigcap_{i:=1}^{r} H_i \leq X^\perp \cap Y = \{0\}.$$

Daher ist

$$P_j := \bigcap_{i:=1,\, i \neq j}^{r} H_i$$

ein Punkt, da ja $\mathrm{Rg}_K(Y) = r$ ist. Ist $y \in P_j$, so ist $f(b_i, y) = 0$ für $i \neq j$ und $f(b_j, y) \neq 0$. Es gibt daher auch ein $c_j \in P_j$ mit $f(b_i, c_j) = \delta_{ij}$. Offenbar ist c_1, $\ldots$, c_r eine Basis von Y. Damit ist a) bewiesen.

b) Ist $\mathrm{Rg}_K(U) = r$, so ist nichts zu beweisen. Es sei also

$$\mathrm{Rg}_K(U) < r.$$

Wegen $U \cap X^\perp = \{0\}$ ist $V = U^\perp + X$. Daher ist

$$\begin{aligned}\mathrm{Rg}_K(V) &= \mathrm{Rg}_K(X) + \mathrm{Rg}_K(U^\perp) - \mathrm{Rg}_K(X \cap U^\perp)\\ &= \mathrm{Rg}_K(X) + \mathrm{Rg}_K(V) - \mathrm{Rg}_K(U) - \mathrm{Rg}_K(X \cap U^\perp)\end{aligned}$$

Hieraus folgt

$$\mathrm{Rg}_K(X) = \mathrm{Rg}_K(U) + \mathrm{Rg}_K(X \cap U^\perp),$$

so dass wegen $\mathrm{Rg}_K(U) < \mathrm{Rg}_K(X)$ die Ungleichung $X \cap U^\perp \neq \{0\}$ gilt. Wäre $U^\perp \leq U + X^\perp$, so wäre $U \geq U^\perp \cap X$ und folglich wäre

$$\{0\} = U \cap X^\perp \geq U^\perp \cap X \cap X^\perp = U^\perp \cap X \neq \{0\}.$$

Dieser Widerspruch zeigt, dass es ein $y \in U^\perp$ gibt mit $y \notin U + X^\perp$. Ist $x \in U^\perp \cap X$, so ist $y + x \in U^\perp$ und wegen $X \leq X^\perp$ auch $y + x \notin U + X^\perp$. Weil $U^\perp \cap X \neq \{0\}$ und außerdem vollständig isotrop bzw. vollständig singulär ist, gibt es nach 6.1 ein $x \in U^\perp \cap X$, so dass $y + x$ isotrop, bzw. singulär ist. Wegen $y + x \notin U + X^\perp$ ist $y + x \neq 0$. Setze

$$U' := U \oplus (y + x)K.$$

Dann ist $\mathrm{Rg}_K(U') = \mathrm{Rg}_K(U) + 1$. Ferner ist U' vollständig isotrop, bzw. vollständig singulär. Wegen $y + x \notin U + X^\perp$ ist

$$\begin{aligned}\mathrm{Rg}_K(U' + X^\perp) &= \mathrm{Rg}_K(U + X^\perp) + 1\\ &= \mathrm{Rg}_K(U) + \mathrm{Rg}_K(X^\perp) + 1\\ &= \mathrm{Rg}_K(U') + \mathrm{Rg}_K(X^\perp),\end{aligned}$$

so dass $\mathrm{Rg}_K(U' \cap X^\perp) = 0$ ist. Folglich ist $U' \cap X^\perp = \{0\}$. Vollständige Induktion liefert nun die Behauptung unter b).

6.3. Korollar. *Ist X ein vollständig isotroper bzw. vollständig singulärer Unterraum von V, so gibt es einen vollständig isotropen bzw. vollständig singulären Unterraum Y von V mit $\mathrm{Rg}_K(Y) = \mathrm{Rg}_K(X)$ und $X \cap Y = \{0\}$, so dass $X + Y$ nicht isotrop bzw. nicht singulär ist.*

Dies folgt mit $U := \{0\}$ aus 6.2.

Aus 6.3 folgt wiederum, dass $2\mathrm{Rg}_K(X) \leq \mathrm{Rg}_K(V)$ ist, falls X ein vollständig isotroper bzw. vollständig singulärer Unterraum von V ist.

6.4. Satz. *Es sei f eine spurwertige, nicht entartete, symmetrische α-Form auf dem K-Vektorraum V, bzw. die der nicht entarteten quadratischen Form Q auf V assoziierte Bilinearform. Ferner seien X_1 und X_2 zwei maximale vollständig isotrope bzw. vollständig singuläre Unterräume von V. Setze $X := X_1 \cap X_2$. Es seien S_1 und S_2 Unterräume mit $X_i = X \oplus S_i$. Schließlich setzen wir $S := S_1 + S_2$. Es gibt dann zwei Unterräume U und W von V mit:*
a) *Die Unterräume $U+X$, S und W sind nicht isotrop und paarweise orthogonal.*
b) *Es ist $V = X \oplus S \oplus U \oplus W$.*
c) *Es gibt keinen von 0 verschiedenen isotropen bzw. singulären Vektor in W.*
d) *U ist vollständig isotrop bzw. vollständig singulär.*
Darüber hinaus ist $\mathrm{Rg}_K(X_1) = \mathrm{Rg}_K(X_2)$, $\mathrm{Rg}_K(U) = \mathrm{Rg}_K(X)$, $\mathrm{Rg}_K(S_1) = \mathrm{Rg}_K(S_2)$ und $\mathrm{Rg}_K(W) = \mathrm{Rg}_K(V) - 2\mathrm{Rg}_K(X_1)$.

Beweis. Ist M ein maximaler vollständig isotroper bzw. vollständig singulärer Unterraum, ist $x \in M^\perp$ und ist x isotrop bzw. singulär, so ist $x \in M$, da andernfalls $M + xK$ ein vollständig isotroper bzw. vollständig singulärer Unterraum von V wäre, der M echt umfasste. Ist also $x \in X_i^\perp$ und ist x isotrop bzw. singulär, so ist $x \in X_i$.

Ist $y \in S_1 \cap S_2^\perp$, so ist $y \in X_1^\perp$, da ja $S_1 \leq X_1 \leq X_1^\perp$ ist. Weil $X \leq X_1$ gilt, ist also $y \in X^\perp$. Somit ist

$$y \in X^\perp \cap S_2^\perp = (X + S_2)^\perp = X_2^\perp.$$

Da y isotrop bzw. singulär ist, ist also $y \in X_2$. Also ist

$$y \in S_1 \cap X_2 = S_1 \cap X_1 \cap X_2 = S_1 \cap X = \{0\}.$$

Somit ist $S_1 \cap S_2^\perp = \{0\}$. Ebenso folgt $S_2 \cap S_1^\perp = \{0\}$.

Weil f nicht entartet ist, ist also, da ja $S_1 \cap S_2^\perp = \{0\}$ ist, $V = S_1 \oplus S_2^\perp$. Also ist

$$\mathrm{Rg}_K(S_1) + \mathrm{Rg}_K(S_2^\perp) = \mathrm{Rg}_K(V).$$

Andererseits ist

$$\mathrm{Rg}_K(S_2) + \mathrm{Rg}_K(S_2^\perp) = \mathrm{Rg}_K(V),$$

so dass

$$\mathrm{Rg}_K(S_1) = \mathrm{Rg}_K(S_2)$$

ist. Hieraus und aus $S_1 \cap S_2^\perp = \{0\}$ folgt nach 6.2 a), dass $S = S_1 + S_2$ nicht isotrop ist. Aus 1.5 folgt weiter, dass $S^\perp$ nicht isotrop ist. Es ist $X \leq S^\perp$. Nach 6.3, angewandt auf X und $S^\perp$, gibt es daher einen vollständig isotropen bzw. vollständig singulären Unterraum $U \leq S^\perp$ mit $\mathrm{Rg}_K(X) = \mathrm{Rg}_K(U)$ und $X \cap U = \{0\}$, so dass $X + U$ nicht singulär ist. Wir setzen

$$W := (X+U)^\perp \cap S^\perp.$$

Weil S nicht isotrop ist, ist $V = S \oplus S^\perp$. Daher ist, da ja $S \leq (X+U)^\perp$ gilt,

$$\begin{aligned}(X+U)^\perp &= (X+U)^\perp \cap (S \oplus S^\perp)\\ &= S \oplus \big((X+U)^\perp \cap S^\perp\big)\\ &= S \oplus W.\end{aligned}$$

Weil $X+U$ und damit $(X+U)^\perp$ nicht isotrop sind und dies auch von S gilt, ist auch W nicht isotrop. Weil ferner $S \leq (X+U)^\perp$, $W \leq S^\perp$ und $X+U \leq W^\perp$ gilt, ist a) erfüllt. Ferner ist

$$V = X \oplus U \oplus (X \oplus U)^\perp = X \oplus U \oplus S \oplus W,$$

so dass auch b) gilt

Es sei $w \in W$ und w sei isotrop bzw. singulär. Dann ist

$$w \in (X+S)^\perp \leq X_1^\perp,$$

so dass nach unserer Bemerkung zu Anfang des Beweises $w \in X_1$ gilt. Daher ist

$$w \in X_1 \cap W \leq (X+S) \cap W = \{0\}.$$

Damit ist auch c) bewiesen.

Wir haben bereits gezeigt, dass

$$\mathrm{Rg}_K(S_1) = \mathrm{Rg}_K(S_2)$$

und

$$\mathrm{Rg}_K(X) = \mathrm{Rg}_K(U)$$

ist. Alle übrigen Rangaussagen folgen aus diesen.

Es sei V ein Vektorraum und f sei eine spurwertige α-Form auf V oder die einer quadratischen Form assoziierte Bilinearform. Sind X, Y und Z Unterräume von V und ist $V = X \oplus Y \oplus Z$, so nennt man diese Zerlegung von V in eine direkte Summe *wittsche Zerlegung von* V, falls X und Y vollständig isotrop bzw. vollständig singulär sind, falls Z nicht isotrop ist und falls $Z \leq (X+Y)^\perp$ gilt.

6.5. Satz. *Es sei f eine spurwertige, nicht ausgeartete symmetrische α-Form auf dem K-Vektorraum V bzw. die der nicht ausgearteten quadratischen Form Q auf V assoziierte Bilinearform. Dann gilt:*

(a) *Sind X und Y zwei maximale vollständig isotrope bzw. vollständig singuläre Teilräume von V, so ist* $\mathrm{Rg}_K(X) = \mathrm{Rg}_K(Y)$.

(b) *Ist X ein maximaler vollständig isotroper bzw. vollständig singulärer Teilraum von V, so gibt es einen maximalen vollständig isotropen bzw. vollständig singulären Teilraum Y von V mit $X \cap Y = \{0\}$.*

(c) *Sind X und Y maximale vollständig isotrope bzw. vollständig singuläre Teilräume mit $X \cap Y = \{0\}$, so ist $X + Y$ nicht isotrop und $(X+Y)^\perp$ enthält keinen von 0 verschiedenen isotropen bzw. singulären Vektor. Insbesondere ist X, Y, $(X+Y)^\perp$ eine wittsche Zerlegung von V.*

(d) *V besitzt eine wittsche Zerlegung.*

Dies folgt unmittelbar aus 6.4 und 6.3.

Ist ν der Rang eines maximalen vollständig isotropen bzw. eines maximalen vollständig singulären Teilraumes von V, so ist ν nach 6.5a) der Rang eines jeden maximalen vollständig isotropen bzw. singulären Teilraumes. Die Zahl ν heißt *Index* von f bzw. von Q. Nach 6.5b) ist $2\nu \leq \mathrm{Rg}_K(V)$. Ist $2\nu = \mathrm{Rg}_K(V)$, so heißt f bzw. Q von *maximalem Index*. Formen von maximalem Index gibt es also höchstens dann, wenn der Rang von V gerade ist. In diesem Falle gibt es aber auch immer eine. Genauer gilt:

6.6. Satz. *Es sei V ein Vektorraum des Ranges 2ν. Dann gibt es bis auf Isometrie genau eine quadratische Form des Index ν auf V.*

Beweis. Es sei Q eine quadratische Form vom Index ν auf V und f sei die zugehörige Bilinearform. Nach 6.3 gibt es dann zwei vollständig singuläre Unterräume X und Y des Ranges ν mit $X \cap Y = \{0\}$, so dass $X + Y$ nicht isotrop ist. Dann ist

$$V = X \oplus Y,$$

da ja $\mathrm{Rg}_K(V) = \mathrm{Rg}_K(X) + \mathrm{Rg}_K(Y)$ ist. Es sei $v \in V$. Es gibt dann $x \in X$ und $y \in Y$ mit $v = x + y$. Es folgt

$$Q(v) = Q(x) + Q(y) + f(x, y) = f(x, y).$$

Wegen $X = X^\perp$ ist $X^\perp \cap Y = \{0\}$, so dass es nach 6.2 eine Basis $b_1, \ldots, b_\nu$ von X und eine Basis $c_1, \ldots, c_\nu$ von Y gibt mit $f(b_i, c_j) = \delta_{ij}$ für alle i und j. Hieraus und aus $Q(v) = f(x, y)$ folgt, dass Q bis auf Isometrie eindeutig festliegt.

Es seien umgekehrt X und Y Unterräume des Ranges ν von V und es gelte $V = X \oplus Y$. Ist $b_1, \ldots, b_\nu$ eine Basis von X und $c_1, \ldots, c_\nu$ eine solche von Y, so definieren wir f durch

$$f(x, y) := \sum_{i:=1}^{\nu} x_i y_i,$$

falls $x = \sum_{i:=1}^{\nu} b_i x_i$ und $y = \sum_{i:=1}^{\nu} c_i y_i$ ist, und weiter durch

$$f(x + y, x' + y') = f(x, y') + f(x', y)$$

für alle x, $x' \in X$ und alle y, $y' \in Y$. Dann ist

$$f(y,x) = f(0+y, x+0) = f(0,0) + f(x,y) = f(x,y).$$

Ferner ist

$$Q((x+y)k) = f(xk, yk) = f(x,y)k^2 = Q(x+y)k^2$$

und

$$\begin{aligned} Q(x+y+x'+y') - Q(x+y) - Q(x'+y') \\ &= f(x+x', y+y') - f(x,y) - f(x',y') \\ &= f(x,y') + f(x',y) = f(x+y, x'+y'). \end{aligned}$$

Damit ist gezeigt, dass Q eine quadratische Form ist, die überdies nicht ausgeartet ist. Weil X und Y vollständig singulär sind, ist ν der Index von Q. Damit ist alles bewiesen.

7. Der Satz von Witt

Der Satz von Witt, den wir in diesem Abschnitt beweisen werden, ist von großer Wichtigkeit beim Studium der Zentralisatoren von Polaritäten. Bevor wir ihn formulieren, jedoch noch einige Bemerkungen. Zunächst erweitern wir den Begriff der Isometrie etwas.

Ist f eine α-Form auf dem K-Vektorraum V und f' eine α-Form auf dem K-Vektorraum V', ist σ eine bijektive lineare Abbildung von V auf V' und gilt $f'(x^\sigma, y^\sigma) = f(x,y)$ für alle x, $y \in V$, so heißt σ *Isometrie* von V auf V'. Ferner nennen wir σ auch dann eine Isometrie von V auf V', wenn Q eine quadratische Form auf V und Q' eine quadratische Form auf V' ist und wenn für alle $x \in V$ die Gleichung $Q'(x^\sigma) = Q(x)$ gilt.

Es sei f eine nicht entartete α-Form auf V und f' sei eine α-Form auf V'. Ferner sei σ eine lineare Abbildung von V in V' mit $f'(x^\sigma, y^\sigma) = f(x,y)$ für alle x, $y \in V$. Ist $y^\sigma = 0$, so ist

$$f(x,y) = f'(x^\sigma, y^\sigma) = f'(x^\sigma, 0) = 0$$

für alle $x \in V$, so dass $y = 0$ ist, da f als nicht entartet vorausgesetzt wurde. Also ist σ injektiv. Ist $\mathrm{Rg}_K(V) = \mathrm{Rg}_K(V')$, so ist σ also eine Bijektion und damit eine Isometrie.

7.1. Satz. *Ist f eine symmetrische α-Form auf V bzw. die zu einer quadratischen Form Q assoziierte Bilinearform, sind ferner X_1 und X_2 Teilräume von V sowie σ_1 und σ_2 Isometrien von X_1 bzw. X_2 in V, gilt*

$$X_1 \cap X_2 = \{0\} = X_1^{\sigma_1} \cap X_2^{\sigma_2}$$

und

$$f(x_1^{\sigma_1}, x_2^{\sigma_2}) = f(x_1, x_2)$$

für alle $x_1 \in X_1$ und alle $x_2 \in X_2$ (dies ist eine zusätzliche Eigenschaft zu den Isometriebedingungen), so ist die durch

$$(x_1 + x_2)^\nu := x_1^{\sigma_1} + x_2^{\sigma_2}$$

definierte lineare Abbildung ν von $X_1 \oplus X_2$ auf $X_1^{\sigma_1} \oplus X_2^{\sigma_2}$ eine Isometrie von $X_1 \oplus X_2$ in V.

Beweis. Es ist banal, dass ν eine bijektive lineare Abbildung von $X_1 \oplus X_2$ auf $X_1^{\sigma_1} \oplus X_2^{\sigma_2}$ ist. Ferner ist

$$\begin{aligned} f\big((x_1 + x_2)^\nu, (y_1 + y_2)^\nu\big) &= f(x_1^{\sigma_1} + x_2^{\sigma_2}, y_1^{\sigma_1} + \sigma_2^{\sigma_2}) \\ &= f(x_1^{\sigma_1}, y_1^{\sigma_1}) + f(x_1^{\sigma_1}, y_2^{\sigma_2}) + f(x_2^{\sigma_2}, y_1^{\sigma_1}) + f(x_2^{\sigma_2}, y^{\sigma_2}) \\ &= f(x_1, y_1) + f(x_1, y_2) + f(x_2, y_1) + f(x_2, y_2) \\ &= f(x_1 + x_2, y_1 + y_2), \end{aligned}$$

bzw.

$$\begin{aligned} Q\big((x_1 + x_2)^\nu\big) &= Q(x_1^{\sigma_1} + x_2^{\sigma_2}) \\ &= Q(x_1^{\sigma_1}) + Q(x_2^{\sigma_2}) + f(x_1^{\sigma_1}, x_2^{\sigma_2}) \\ &= Q(x_1) + Q(x_2) + f(x_1, x_2) \\ &= Q(x_1 + x_2). \end{aligned}$$

Damit ist gezeigt, dass ν eine Isometrie ist.

7.2. Satz von Witt. *Es sei f eine spurwertige, symmetrische, nicht entartete α-Form auf dem K-Vektorraum V, bzw. die der nicht entarteten quadratischen Form Q auf V assoziierte Bilinearform. Ist X ein Teilraum von V und ist σ eine injektive lineare Abbildung von X in V mit $f(x^\sigma, y^\sigma) = f(x, y)$ für alle x, $y \in X$, bzw. $Q(x^\sigma) = Q(x)$ für alle $x \in X$, so gibt es eine Isometrie τ von V auf sich mit $x^\tau = x^\sigma$ für alle $x \in X$.*

Beweis. Setze

$$Y := \{y \mid y \in X, y^\sigma = y\} \quad \text{und} \quad P := \{x^\sigma - x \mid x \in X\}.$$

Dann ist $P \cong X/Y$.

Wir betrachten zunächst den Fall, wo Y eine Hyperebene von X ist. Wegen $P \cong X/Y$ ist P dann ein Punkt.

Ist $X' \leq P^\perp$ und $X \cap X' = X^\sigma \cap X' = \{0\}$, so gilt für $x \in X$ und $y \in X'$ wegen $X' \leq P^\perp$ die Gleichung

$$0 = f(x^\sigma - x, y) = f(x^\sigma, y) - f(x, y),$$

so dass $f(x^\sigma, y) = f(x, y)$ ist. Definiert man ν durch

$$(x + y)^\nu := x^\sigma + y,$$

so ist ν nach 7.1 eine Isometrie von $X \oplus X'$ in V, die überdies die Vektoren aus X' festlässt. Hieraus folgt weiter

$$P = \{x^\nu - x \mid x \in X + X'\}.$$

Sind x, $y \in X$, so ist

$$(*) \quad f(x^\sigma, y^\sigma - y) = f(x^\sigma, y^\sigma) - f(x^\sigma, y) = f(x, y) - f(x^\sigma, y) = f(x - x^\sigma, y).$$

Ist überdies $x \in Y$, so ist nach $(*)$ also

$$f(x, y^\sigma - y) = f(x^\sigma, y^\sigma - y) = f(x - x^\sigma, y) = 0,$$

da in diesem Falle ja $x = x^\sigma$ ist. Also ist $Y \leq P^\perp$.

1. Fall: Es ist $X \not\leq P^\perp$. Aus $(*)$ folgt, dass dann auch $X^\sigma \not\leq P^\perp$ ist. Weil Y eine Hyperebene von X und damit auch von X^σ ist und weil

$$Y \leq X \cap P^\perp, \ X^\sigma \cap P^\perp$$

gilt, ist also

$$X \cap P^\perp = Y = X^\sigma \cap P^\perp.$$

Wähle ein Komplement X' von Y in $P^\perp$. Dann ist $X \cap X' = \{0\}$ und $X^\sigma \cap X' = \{0\}$, so dass sich σ, wie eingangs bemerkt, zu einer Isometrie ν von $X + X'$ in V fortsetzen lässt. Nun ist

$$P^\perp = Y \oplus X' < X + X' \leq V,$$

so dass $X + X' = V$ ist, da $P^\perp$ ja eine Hyperebene von V ist. In diesem Falle setze man $\tau := \nu$. Dann ist τ eine mögliche Fortsetzung von σ.

2. Fall: Es ist $X \leq P^\perp$. Aus $(*)$ folgt, dass dann auch $X^\sigma \leq P^\perp$ ist. Hieraus folgt weiter

$$P \leq X + X^\sigma \leq P^\perp,$$

so dass P isotrop bzw. singulär ist. Für Letzteres muss man noch beachten, dass für $p \in P$ die Gleichung $Q(p) = 0$ gilt. Ist $p \in P$, so gibt es ein $x \in X$ mit $p = x^\sigma - x$ und es folgt

$$Q(x^\sigma - x) = Q(x^\sigma) + Q(x) - f(x^\sigma, x) = 2Q(x) - f(x^\sigma - x, x) - f(x, x) = 0.$$

Nach I.7.2 gibt es einen Teilraum X' von $P^\perp$ mit

$$X \oplus X' = P^\perp = X^\sigma \oplus X'.$$

Nach 7.1 lässt sich σ zu einer Isometrie von $X \oplus X'$ auf $X^\sigma \oplus X'$, dh. zu einer Isometrie von $P^\perp$ fortsetzen, die überdies die Hyperebene $Y + X'$ von $P^\perp$ elementweise festlässt. Wir dürfen daher im weiteren Verlauf des Beweises annehmen, dass $X = P^\perp$ ist und dass σ eine Isometrie von X auf sich ist. Dies wird im Folgenden wesentlich benutzt.

Ist $z \in V$, so ist die Abbildung $x \to f(x^{\sigma^{-1}}, z)$ für $x \in X$ eine lineare Abbildung von X in K. Es gibt ferner eine lineare Abbildung φ von V in K mit $\varphi(x) = f(x^{\sigma^{-1}}, z)$ für alle $x \in X$. Weil f nicht ausgeartet ist, gibt es ein $z' \in V$ mit $f(v, z') = \varphi(v)$ für alle $v \in V$. Ersetzt man x durch x^σ, so sieht man, dass es zu jedem $z \in V$ ein $z' \in V$ gibt mit

$$f(x, z) = \varphi(x^\sigma) = f(x^\sigma, z')$$

für alle $x \in X$. Ist $y \in X$, so gilt wegen $X = X^\sigma = P^\perp$ die Gleichung

$$(**) \qquad f(x^\sigma, z') = f(x^\sigma, z' + y^\sigma - y).$$

Ist $z \notin X$, so ist auch $z' \notin X$. Wäre nämlich $z' \in X$, so wäre

$$f(x^\sigma - x, z') = 0$$

für alle $x \in X$, woraus $f(x^\sigma, z') = f(x, z)$ für alle $x \in X$ folgte. Daher gälte nach $(**)$ die Gleichung $f(x, z') = f(x, z)$ für alle $x \in X$, was wiederum $f(x, z - z') = 0$ nach sich zöge, so dass

$$z - z' \in X^\perp = P^{\perp\perp} = P \leq X$$

wäre im Widerspruch zu $z \notin X$. Da P vollständig isotrop bzw. vollständig singulär ist und weil f als spurwertig vorausgesetzt wurde, gibt es nach 6.1 ein $y \in X$ mit

$$f(z' + y^\sigma - y, z' + y^\sigma - y) = f(z, z)$$

bzw.

$$Q(z' + y^\sigma - y) = Q(z).$$

Weil schließlich

$$f(x^\sigma, z') = f(x^\sigma, z' + y^\sigma - y)$$

für alle $x \in X$ gilt, ersetzen wir z' durch $z' + y^\sigma - y$ um zu sehen, dass es zu $z \in V$ mit $z \notin X$ ein $z' \in V$ mit $z' \notin X$ gibt, so dass

$$f(x^\sigma, z') = f(x, z')$$

für alle $x \in X$ gilt, sowie

$$f(z', z') = f(z, z)$$

bzw.

$$Q(z') = Q(z).$$

Hieraus folgt, dass sich σ zu einer Isometrie von $X \oplus zK = V$ auf $X \oplus z'K = V$ fortsetzen lässt.

Der Rest des Beweises folgt nun mit Induktion nach $\mathrm{Rg}_K(X)$. Ist $\mathrm{Rg}_K(X) = 0$, so ist der Satz trivial. Es sei also $n := \mathrm{Rg}_K(X) > 0$ und $Z \leq X$ sowie $\mathrm{Rg}_K(Z) = n-1$. Schränkt man σ auf Z ein, so gibt es nach Induktionsannahme eine Isometrie ρ von V mit $y^\sigma = y^\rho$ für alle $y \in Z$. Ist sogar $x^\sigma = x^\rho$ für alle $x \in X$, so ist $\tau := \rho$ eine Fortsetzung von σ auf V. Es sei also $x^\rho \neq x^\sigma$ für wenigstens ein $x \in X$. Dann ist $\sigma\rho^{-1}$ eine Isometrie von X in V mit

$$Z = \{x \mid x \in X, x^{\sigma\rho^{-1}} = x\}.$$

Nach dem bereits Bewiesenen — Z spielt jetzt die Rolle von Y — gibt es dann eine Isometrie ν von V mit $x^\nu = x^{\sigma\rho^{-1}}$ für alle $x \in X$. Die Abbildung $\tau := \nu\rho$ ist dann eine Isometrie von V mit $x^\sigma = x^\tau$ für alle $x \in X$. Damit ist 7.2 bewiesen.

7.3. Korollar. *Es sei f eine spurwertige, nicht entartete α-Form auf dem Vektorraum V, bzw. die der nicht entarteten quadratischen Form Q auf V assoziierte Bilinearform. Ist dann G die Gruppe der zugehörigen Isometrien, so gilt:*

a) *Ist M die Menge der vollständig isotropen, bzw. vollständig singulären Unterräume vom Rang i von V, so ist G auf M transitiv.*

b) *Ist U ein vollständig isotroper bzw. vollständig singulärer Unterraum von V, so wird jede Isometrie von U auf sich von einem $\sigma \in G$ induziert.*

Dies folgt unmittelbar aus 7.2.

8. Unitäre Gruppen

Als Nächstes studieren wir die Zentralisatoren von unitären Polaritäten, die durch spurwertige α-Formen dargestellt werden. Das uns hier vor allem interessierende Resultat ist, dass die von Elationen erzeugte Untergruppe einer solchen Gruppe bis auf drei Ausnahmen einfach ist. Wir werden diesen Satz nicht in voller Allgemeinheit beweisen, aber nur solche Geometrien ausschließen, deren Koordinatenkörper nicht kommutativ sind und ein Zentrum haben, welches zu GF(2), GF(3), GF(4) oder GF(9) isomorph ist. Dass wir diese sehr fremdartigen Körper aus der Betrachtung ausschließen, liegt an unserer Beweismethode. Es gibt zwar Schiefkörper, deren Zentrum zu einem der genannten Galoisfelder isomorph ist (P. M. Cohn 1977, S. 116/117), ich weiß aber nicht, ob es unter ihnen auch solche gibt, die einen Antiautomorphismus gestatten. Das Studium der unitären Gruppen wird uns drei Abschnitte lang beschäftigen.

Bei den Studien dieses Abschnitts werden wir uns des Satzes 1.9 bedienen, der besagt, dass sich unitäre Polaritäten nicht nur durch symmetrische α-Formen, sondern auch durch antisymmetrische α-Formen darstellen lassen. Dabei heißt eine α-Form *antisymmetrisch*, falls

$$f(u,v)^\alpha = -f(v,u)$$

ist für alle u, $v \in V$ und falls im Falle $\alpha = 1$ außerdem $f(x,x) = 0$ für alle $x \in V$ gilt. Dies hat den Vorteil, dass die hier vorzutragenden Sätze auch für die symplektischen Gruppen gelten. Dies werden wir nicht weiter ausnutzen, da wir die Einfachheit der symplektischen Gruppen ja bereits bewiesen haben.

8.1. Satz. *Es sei V ein Vektorraum über dem Körper K und f sei eine nicht ausgeartete, antisymmetrische α-Semibilinearform auf V. Ferner sei φ eine lineare Abbildung von V in K und h sei ein Element des Kernes von φ. Ist τ die durch*

$$x^\tau := x + h\varphi(x)$$

definierte Transvektion von V, so ist τ genau dann eine Isometrie von V, wenn es ein $\lambda \in K$ gibt mit $\lambda^\alpha = \lambda$ und

$$\varphi(x) = \lambda f(h,x)$$

für alle $x \in V$.

Transvektionen dieser Art nennen wir in Zukunft *unitär*.

Beweis. Wir dürfen annehmen, dass $\tau \neq 1$ ist. Es sei τ eine Isometrie. Dann ist

$$\begin{aligned} f(u,v) &= f(u^\tau, v^\tau) = f(u + h\varphi(u), v + h\varphi(v)) \\ &= f(u,v) + f(u,h)\varphi(u) + \varphi(u)^\alpha f(h,v) + \varphi(u)^\alpha f(h,h)\varphi(v) \end{aligned}$$

für alle u, $v \in V$. Es folgt

$$0 = f(u,h)\varphi(v) + \varphi(u)^\alpha f(h,v) + \varphi(u)^\alpha f(h,h)\varphi(v)$$

für alle u, $v \in V$. Setze $u := h$. Dann ist

$$0 = f(h,h)\varphi(v) + 0^\alpha f(h,v) + 0^\alpha f(h,h)\varphi(v) = f(h,h)\varphi(v)$$

für alle $v \in V$. Wegen $\tau \neq 1$ gibt es ein $v \in V$ mit $\varphi(v) \neq 0$, so dass $f(h,h) = 0$ ist.

Wegen $f(h,h) = 0$ ist

$$0 = f(u,h)\varphi(v) + \varphi(u)^\alpha f(h,v)$$

für alle u, $v \in V$. Da f nicht entartet ist und wegen $\tau \neq 1$ auch $h \neq 0$ gilt, gibt es ein $u \in V$ mit $f(u,h) = 1$. Es folgt

$$\varphi(v) = -\varphi(u)^\alpha f(h,v)$$

für alle $v \in V$. Setze $\lambda := -\varphi(u)^\alpha$. Dann ist also $\varphi(v) = \lambda f(h,v)$ für alle $v \in V$. Es folgt

$$\varphi(u) = \lambda f(h,u) = \lambda\big(-f(u,h)^\alpha\big) = -\lambda = \varphi(u)^\alpha.$$

Hieraus folgt wiederum $\lambda^\alpha = \lambda$.

Ist umgekehrt $\lambda^\alpha = \lambda$ und $f(h,h) = 0$, so zeigt eine banale Rechnung, dass die durch $x^\tau := x + h\lambda f(h,x)$ definierte Transvektion τ eine Isometrie ist.

8.2. Satz. *Es sei V ein Vektorraum über dem Körper K und f sei eine nicht ausgeartete, antisymmetrische α-Form auf V. Ist P ein isotroper Punkt, ist G eine nicht isotrope Gerade durch P und sind Q und R von P verschiedene isotrope Punkte auf G, so gibt es eine unitäre Transvektion τ mit dem Zentrum P, für die $Q^\tau = R$ gilt.*

Beweis. Es sei $P = pK$, $Q = qK$ und $R = rK$. Dann sind die Vektoren p, q und r isotrop. Da G nicht isotrop ist, ist $f(p,q)$, $f(p,r) \neq 0$. Indem man q und r ggf. mit einem Skalar multipliziert, kann man erreichen, dass $f(p,q) = f(p,r) = 1$ ist. Weil p und q linear unabhängig sind, gibt es μ und λ mit $r = p\lambda + q\mu$. Es folgt

$$1 = f(p,r) = f(p, p\lambda + q\mu) = \mu$$

und

$$0 = f(r,r) = f(p\lambda + q, p\lambda + q) = \lambda^\alpha f(p,q) + f(q,p)\lambda = \lambda^\alpha - \lambda.$$

Also ist $\lambda^\alpha = \lambda$. Definiert man nun τ durch

$$x^\tau := x + p\lambda f(p, x),$$

so ist τ nach 8.1 eine unitäre Transvektion mit dem Zentrum P und es gilt

$$q^\tau = q + p\lambda = r,$$

so dass $Q^\tau = R$ ist. Damit ist alles bewiesen.

Ist g eine spurwertige, nicht ausgeartete, symmetrische α-Form mit $\alpha \neq 1$, so gibt es nach Satz 1.9 eine nicht ausgeartete, antisymmetrische β-Form f und ein $k \in K^*$ mit $f(u, v) = kg(u, v)$. Die Isometrien von f sind offenbar die gleichen wie die von g. Ist g spurwertig, so können wir die Sätze über spurwertige α-Formen auch auf f anwenden. Um dies auszudrücken werden wir auch f *spurwertig* nennen, wenn der gerade geschilderte Zusammenhang besteht.

8.3. Satz. *Es sei f eine nicht ausgeartete, antisymmetrische, spurwertige α-Form auf dem K-Vektorraum V. Mit Σ bezeichnen wir die Elemente $s \in K$, für die $s^\alpha = s$ gilt. Es sei G eine nicht isotrope Gerade von $\mathrm{L}(V)$ und P sei ein isotroper Punkt auf G. Es gibt dann einen weiteren isotropen Punkt Q auf G. Ist dann $P = pK$ und $Q = qK$, so ist*

$$\{(q + ps)K \mid s \in \Sigma\}$$

die Menge der von P verschiedenen isotropen Punkte auf G. Überdies gilt: Ist $(q + ps)K = (q + pt)K$, so ist $s = t$. Insbesondere gilt, dass G mindestens drei isotrope Punkte trägt.

Beweis. Weil G nicht isotrop ist, ist die Einschränkung von f auf G nicht ausgeartet. Nach 6.3 gibt es daher einen isotropen Punkt Q von G mit $G = P + Q$. Wiederum weil G nicht isotrop ist, gilt $f(p, q) \neq 0$, falls $0 \neq p \in P$ und $0 \neq q \in Q$ ist. Daher gibt es ein $p \in P$ und ein $q \in Q$ mit $f(p, q) = 1$. Ist nun R ein von P verschiedener isotroper Punkt auf G, so gibt es, wie wir beim Beweise von 8.2 gesehen haben, ein $r \in \Sigma$ mit $R = (q + pr)K$. Daher ist R in der Menge

$$\{(q + ps)K \mid s \in \Sigma\}$$

enthalten. Ist andererseits $s \in \Sigma$, so folgt

$$\begin{aligned} f(q + ps, q + ps) &= f(q, ps) + f(ps, q) = f(q, ps) - f(q, ps)^\alpha \\ &= f(p, q)s - \big(f(p, q)s\big)^\alpha = s - s^\alpha = 0. \end{aligned}$$

Also ist $\{(q + ps)K \mid s \in \Sigma\}$ in der Tat die Menge der isotropen Punkte auf G.

Sind s, $t \in \Sigma$ und gilt $(q + ps)K = (q + pt)K$, so folgt $s = t$, da p und q ja linear unabhängig sind.

Die letzte Aussage des Satzes folgt schließlich daraus, dass Σ zumindest die beiden Elemente 0 und 1 enthält.

Ist f eine nicht ausgeartete, antisymmetrische oder auch eine nicht ausgeartete, symmetrische α-Form auf dem Vektorraum V, so bezeichnen wir mit

$\mathrm{U}(V, f)$ die Gruppe aller Isometrien von f und mit $\mathrm{TU}(V, f)$ die von allen bez. f unitären Transvektionen erzeugte Untergruppe von $\mathrm{U}(V, f)$.

8.4. Satz. *Es sei f eine nicht ausgeartete, antisymmetrische, spurwertige α-Form auf dem K-Vektorraum V, deren Index mindestens 1 sei. Dann ist die Gruppe $\mathrm{TU}(V, f)$ auf der Menge der isotropen Punkte von $\mathrm{L}(V)$ transitiv.*

Beweis. Es seien $P = pK$ und $Q = qK$ zwei verschiedene isotrope Punkte von $\mathrm{L}(V)$. Ist $f(p, q) \neq 0$, so ist $P + Q$ eine nicht isotrope Gerade. Es gibt daher nach 8.3 einen dritten isotropen Punkt R auf G. Nach 8.2 gibt es dann eine Transvektion mit dem Zentrum R, die P auf Q abbildet.

Ist $f(p, q) = 0$, so ist $P + Q$ vollständig isotrop. Nach dem Korollar 6.3 gibt es einen vollständig isotropen Unterraum U von V mit $U \cap (P + Q)^\perp = \{0\}$. Nach 8.2 a) gibt es ferner eine Basis p', q' von U mit $f(p, p') = 1 = f(q, q')$ und $f(p, q') = 0 = f(q, p')$. Dann ist $(p' + q')K$ ein isotroper Punkt und es gilt

$$f(p, p' + q') = 1 = f(q, p' + q'),$$

so dass es, wie soeben gezeigt, eine unitäre Transvektion gibt, die P auf $(p' + q')K$ abbildet, und eine unitäre Transvektion, die $(p' + q')K$ auf Q abbildet. Damit ist alles gezeigt.

Im Folgenden benutzen wir Techniken, die wir schon beim Beweise der Einfachheit der kleinen projektiven Gruppe in Abschnitt 2 des Kapitels II benutzt haben. Hier sind es insbesondere die Sätze II.2.4 und II.2.5, die sich ohne Mühe auf den vorliegenden Fall übertragen lassen.

8.5. Satz. *Es sei f eine nicht ausgeartete, antisymmetrische α-Form auf dem K-Vektorraum V. Es seien u und v zwei isotrope Vektoren mit $f(u, v) = 1$. Ferner sei $a \in K^*$ und es gelte $a^\alpha = a$. Nach 8.1 werden dann durch*

$$\begin{aligned} x^{\tau_1} &:= x - uf(u, x), \\ x^{\tau_2} &:= x - v(1 - a)a^{-1}f(v, x), \\ x^{\tau_3} &:= x - uaf(u, x), \\ x^{\tau_4} &:= x - v(1 - a)a^{-2}f(v, x) \end{aligned}$$

vier unitäre Transvektionen τ_i definiert. Setze

$$\sigma := \tau_1\tau_2\tau_3\tau_4.$$

Dann ist $u^\sigma = ua$, $v^\sigma = va^{-1}$ und $x^\sigma = x$ für alle $x \in (uK + vK)^\perp$.

Beweis. Wie schon bei Satz III.2.4 sage ich auch hier: Rechnen!

8.6. Satz. *Es sei f eine nicht ausgeartete, antisymmetrische α-Form auf dem K-Vektorraum V. Es seien u und v zwei isotrope Vektoren aus V mit $f(u, v) = 1$. Ferner seien a, $b \in K^*$ und es gelte $a^\alpha = a$ und $b^\alpha = b$. Wir definieren σ, $\tau \in \mathrm{TU}(V, f)$ durch*

$$(uk + vl + x)^\sigma := uak + va^{-1}l + x$$

für alle k, $l \in K$ und alle $x \in (uK + vK)^\perp$ sowie

$$x^\tau = x + vbf(v, x)$$

für alle $x \in V$. Dann ist

$$x^{\sigma^{-1}\tau^{-1}\sigma\tau} = x + v(b - a^{-1}ba^{-1})f(v, x).$$

Beweis. Dass τ eine unitäre Transvektion ist, folgt aus Satz 8.1, und dass $\sigma \in \mathrm{TU}(V, f)$ ist, aus Satz 8.5.

Es ist $(a^{-1})^\alpha = a^{-1}$ und σ ist eine Isometrie. Daher ist

$$\begin{aligned} x^{\sigma^{-1}\tau^{-1}\sigma\tau} &= (x^{\sigma^{-1}} - vbf(v, x^{\sigma^{-1}}))^{\sigma\tau} \\ &= (x - va^{-1}bf(v, x^{\sigma^{-1}}))^\tau \\ &= \big(x - va^{-1}ba^{-1}f(v^{\sigma^{-1}}, x^{\sigma^{-1}})\big)^\tau \\ &= x + vbf(v, x) - va^{-1}ba^{-1}f(v, x), \end{aligned}$$

q. o. o.

Um diesen Satz erfolgreich anwenden zu können, müssen wir wissen, wann es in einem Körper K von Null verschiedene Elemente a gibt mit $a^\alpha = a$ und $a^2 \neq 1$. Darüber gibt der nächste Satz Auskunft.

8.7. Satz. *Es sei K ein Körper und α sei ein Antiautomorphismus mit $\alpha^2 = 1$. Setze*

$$L := \{a \mid a \in K, a^\alpha = a\}.$$

Gilt $a^2 = 1$ für alle $a \in L - \{0\}$, so ist $L = \mathrm{GF}(2)$ oder $\mathrm{GF}(3)$ und $[K : L] \leq 2$.

Beweis. Es sei $0 \neq a \in L$. Dann ist $(a - 1)(a + 1) = a^2 - 1 = 0$ und daher $a = 1$ oder -1. Also ist $L = \{0, 1, -1\}$. Folglich liegt L im Zentrum $Z(K)$ von K. Weil α in $Z(K)$ einen Automorphismus induziert, ist L ein Teilkörper von $Z(K)$. Ist nun $k \in K$, so ist

$$(k + k^\alpha)^\alpha = k^\alpha + k^{\alpha^2} = k + k^\alpha,$$

so dass $k + k^\alpha \in L$ gilt für alle $k \in K$. Weil α ein Antiautomorphismus ist, folgt

$$(k^\alpha k)^\alpha = k^\alpha k^{\alpha^2} = k^\alpha k,$$

so dass auch $k^\alpha k \in L$ gilt. Nun ist[3]

$$k^2 - (k + k^\alpha)k + k^\alpha k = 0.$$

[3] Anmerkung der Herausgeber: Für $a, b \in K$ folgt aus dieser Beziehung $ab + ba = (a+b)^2 - a^2 - b^2 \in L + La + Lb$, und $L + La + Lb + Lab$ enthält ba und ist ein Teilring, also ein endlicher Teilkörper von K (mit 2^4 oder 3^4 Elementen) und daher kommutativ (nach Wedderburn, oder man betrachte ein Element der multiplikativen Ordnung 5). Also ist K kommutativ.

Ist also $k \notin L$, so hat das Minimalpolynom von k über L den Grad 2. Nach Satz II.10.6 ist K dann kommutativ oder es ist $Z(K) = L$ und K ist ein Quaternionenschiefkörper über L. Weil L endlich ist, wäre im letzteren Fall K ein endlicher, nicht kommutativer Körper im Widerspruch zum Satz von Wedderburn, dass alle endlichen Körper kommutativ sind. Also ist K kommutativ, und es folgt $[K : L] \leq 2$, da L ja der Fixkörper von α ist. Nun ist aber $L = \{0, 1, -1\}$ und folglich $L = \mathrm{GF}(2)$ oder $\mathrm{GF}(3)$. Damit ist alles bewiesen.

8.8. Satz. *Es sei K ein Körper und f sei eine nicht ausgeartete, spurwertige, antisymmetrische α-Form auf dem K-Vektorraum V. Der Fixkörper des von α auf $Z(K)$ induzierten Automorphismus sei von* $\mathrm{GF}(2)$ *und* $\mathrm{GF}(3)$ *verschieden. Ist dann der Index von f mindestens* 1, *so ist* $\mathrm{TU}(V, f)' = \mathrm{TU}(V, f)$, *dh.,* $\mathrm{TU}(V, f)$ *ist perfekt.*

Die Voraussetzungen an K sind sicher dann erfüllt, wenn $Z(K)$ von $\mathrm{GF}(2)$, $\mathrm{GF}(3)$, $\mathrm{GF}(4)$ und $\mathrm{GF}(9)$ verschieden ist.

Beweis. Es sei τ eine von 1 verschiedene unitäre Transvektion. Es gibt dann einen isotropen Vektor v und ein $c \in K^*$ mit $c^\alpha = c$, so dass

$$x^\tau = x + vcf(v, x)$$

ist für alle $x \in V$. Weil f nicht ausgeartet ist, gibt es eine nicht isotrope Gerade G durch vK, und weil f spurwertig ist, gibt es einen von vK verschiedenen isotropen Punkt uK auf G. Dann ist $f(u, v) \neq 0$, so dass wir annehmen dürfen, dass $f(u, v) = 1$ ist.

Weil α das Zentrum von K invariant lässt, folgt mit 8.7, dass es ein $a \in Z(K)^*$ gibt mit $a^\alpha = a$ und $a^2 \neq 1$. Setze

$$b := c(1 - a^{-2})^{-1}.$$

Dann ist auch $b^\alpha = b$. Nun ist

$$x^\tau = x + vcf(v, x) = x + vb(1 - a^{-2})f(v, x) = x + v(b - a^{-1}ba^{-1})f(v, x),$$

so dass τ nach 8.6 ein Kommutator ist. Weil also alle Transvektionen Kommutatoren sind, ist $\mathrm{TU}(V, f)$ perfekt.

Dass $\mathrm{TU}(V, f)$ nicht immer perfekt ist, zeigt der folgende Satz.

8.9. Satz. *Es sei K ein kommutativer Körper und V sei ein Vektorraum des Ranges* 2 *über K. Ist dann f eine nicht ausgeartete, spurwertige, antisymmetrische α-Form auf V, deren Index mindestens* 1 *ist, so ist* $\mathrm{TU}(V, f)$ *zu* $\mathrm{SL}(2, L)$ *isomorph. Dabei ist L der durch*

$$L := \{a \mid a \in K, a^\alpha = a\}$$

definierte Teilkörper von K.

Beweis. Weil K kommutativ ist, ist α ein Automorphismus von K, so dass L in der Tat ein Teilkörper ist.

Weil f spurwertig ist und weil der Index von f mindestens 1 ist, gibt es zwei isotrope Vektoren u und v mit $f(u,v) = 1$. Die von den Transvektionen τ der Form

$$x^\tau = x + uaf(u,x)$$

bzw.

$$x^\tau = x + vaf(u,x)$$

mit $a \in L$ erzeugte Untergruppe U von $\mathrm{TU}(V,f)$ ist offensichtlich isomorph zu $\mathrm{SL}(2,L)$. Andererseits operiert sie auf den Punkten von $\mathrm{L}(V)$ transitiv und enthält daher alle Elationen von $\mathrm{TU}(V,f)$. Also ist $U = TU(V,f)$. Damit ist alles bewiesen.

Weil die Gruppen $\mathrm{SL}(2,2)$ und $\mathrm{SL}(2,3)$ auflösbar sind, zeigt 8.9, dass 8.8. nicht ohne Einschränkung an den Körper gültig ist. Wir werden noch sehen, dass $\mathrm{TU}(V,f)$ auch dann nicht perfekt ist, wenn $K = \mathrm{GF}(4)$ und $\mathrm{Rg}_{\mathrm{GF}(4)}(V) = 3$ ist. Dies sind im übrigen alle Ausnahmen.

8.10. Satz. *Es sei f eine nicht ausgeartete, antisymmetrische, spurwertige α-Form auf dem K-Vektorraum V. Ferner sei $\mathrm{Rg}_K(V) \geq 3$ und der Index von f sei mindestens 1. Ist P ein nicht isotroper Punkt von $\mathrm{L}(V)$, so gibt es zwei nicht isotrope Geraden durch P, die je zwei isotrope Punkte tragen.*

Beweis. Es gibt nach Voraussetzung einen isotropen Punkt Q. Es ist $Q \neq P$, so dass $P+Q$ eine Gerade ist. Es gibt einen Punkt R mit $R \not\leq P+Q$, $P^\perp$, $Q^\perp$. Wäre dies nicht der Fall, so enthielten $P+Q$, $P^\perp$ und $Q^\perp$ alle Punkte von $\mathrm{L}(V)$. Dies hätte $\mathrm{Rg}_K(V) = 3$ und $|K| = 2$ zur Folge. Wegen $|K| = 2$ wäre $\alpha = 1$, so dass f eine symplektische Polarität induzierte. Mit Satz 1.7 erhielten wir den Widerspruch, dass $3 = \mathrm{Rg}_K(V)$ gerade wäre. Wir betrachten die Gerade $Q+R$. Wegen $Q \leq Q^\perp$ und $R \cap Q^\perp = \{0\}$ ist dann

$$(Q+R)^\perp \cap (Q+R) = R^\perp \cap Q^\perp \cap (Q+R) = R^\perp \cap Q.$$

Wegen $R \cap Q^\perp = \{0\}$ ist $Q + R^\perp = V$. Da Q ein Punkt und $R^\perp$ eine Hyperebene ist, folgt $Q \cap R^\perp = \{0\}$. Damit ist gezeigt, dass $Q+R$ nicht isotrop ist. Weil Q ein isotroper Punkt auf $Q+R$ ist, folgt mit 8.3, dass $Q+R$ noch zwei von Q verschiedene isotrope Punkte Q' und Q'' trägt. Von den drei Punkten Q, Q' und Q'' liegen wenigstens zwei nicht in $P^\perp$. Wir dürfen annehmen, dass dies die Punkte Q und Q' sind. Dann sind aber die Geraden $P+Q$ und $P+Q'$ nicht isotrop. Es ist ja

$$\begin{aligned}(P+Q)^\perp \cap (P+Q) &= P^\perp \cap Q^\perp \cap (P+Q) \\ &= P^\perp \cap (Q + (P \cap Q^\perp)) = P^\perp \cap Q = \{0\}.\end{aligned}$$

Ebenso folgt, dass auch

$$(P+Q')^\perp \cap (P+Q') = \{0\}$$

ist. Da die beiden Geraden $P+Q$ und $P+Q'$ nicht isotrop sind, enthalten sie nach 8.3 noch je einen weiteren isotropen Punkt. Damit ist der Satz bewiesen.

8.11. Satz. *Es sei f eine nicht ausgeartete, antisymmetrische, spurwertige α-Form auf dem K-Vektorraum V. Ferner sei $\mathrm{Rg}_K(V) \geq 2$ und der Index von f sei mindestens* 1. *Es sei* Π *die Menge der isotropen Punkte von f. Ist dann N der Normalteiler von* $\mathrm{TU}(V,f)$, *der aus allen Abbildungen von* $\mathrm{TU}(V,f)$ *besteht, die alle Punkte von* Π *in sich abbilden, so ist*

$$Z(\mathrm{TU}(V,f)) = N = \mathrm{TU}(V,f) \cap Z(\mathrm{GL}(V)).$$

Beweis. Nach III.1.2 gilt $\mathrm{TU}(V,f) \cap Z(\mathrm{GL}(V)) \subseteq N$. Um die umgekehrte Inklusion zu etablieren, sei zunächst $\mathrm{Rg}_K(V) \geq 3$. Es sei $\nu \in N$ und P sei ein Punkt von $\mathrm{L}(V)$. Ist $P \in \Pi$, so ist $P^\nu = P$ nach Voraussetzung. Es sei also $P \notin \Pi$. Nach 8.10 gibt es dann zwei Geraden G und H durch P, die beide zwei isotrope Punkte tragen. Es folgt $G^\nu = G$ und $H^\nu = H$ und damit $P^\nu = P$. Damit ist gezeigt, dass ν alle Punkte von $\mathrm{L}(V)$ invariant lässt. Mit Satz III.1.2 folgt nun die Behauptung in diesem Falle.

Es sei $\mathrm{Rg}_K(V) = 2$. Es gibt dann eine Basis b_1 und b_2 aus isotropen Vektoren mit $f(b_1, b_2) = 1$. Ist $\lambda \in K$ und $\lambda^\alpha = \lambda$, so wird durch

$$v^\tau := v - b_1\lambda f(b_1, v)$$

eine unitäre Transvektion definiert, wie wir wissen. Es folgt, dass

$$b_2^\tau = b_2 - b_1\lambda f(b_1, b_2) = b_2 - b_1\lambda$$

ein isotroper Vektor ist.

Es sei $\nu \in N$. Es gibt dann r_1, r_2, $r \in K^*$ mit $b_1^\nu = b_1 r_1$, $b_2^\nu = b_2 r_2$ und $b_2^{\tau\nu} = b_2^\tau r = (b_2 - b_1\lambda)r$. Es folgt

$$b_2 r_2 - b_1 r_1 \lambda = b_2^\nu - b_1^\nu \lambda = (b_2 - b_1\lambda)^\nu = b_2^{\tau\nu} = b_2 r - b_1 \lambda r$$

und damit $r_2 = r$ und $r_1\lambda = \lambda r$. Daher ist

$$r_1\lambda = \lambda r_2.$$

Weil r_1 und r_2 von λ unabhängig sind, gilt diese Gleichung für alle $\lambda \in K$, für die $\lambda^\alpha = \lambda$ gilt. Mit $\lambda = 1$ folgt $r_2 = r_1 = r$, womit gleichzeitig gezeigt ist, dass r nicht von λ abhängig ist. Wegen $r\lambda = \lambda r$ für alle λ mit $\lambda^\alpha = \lambda$ ist r nach III.10.11 ein Element des Zentrums von K, es sei denn, es ist K ein Quaternionenschiefkörper mit von 2 verschiedener Charakteristik und es ist

$$Z(K) = \{\lambda \mid \lambda \in K, \lambda^\alpha = \lambda\}.$$

Ist nun T_1 die Menge aller unitären Transvektionen der Form $v^\rho = v - b_1\lambda f(b_1, v)$ und T_2 die Menge aller Transvektionen der Form $v^\tau = v - b_2\mu f(b_2, v)$ mit λ, $\mu \in Z(K)$, so folgt mit 8.2, dass die von T_1 und T_2 erzeugte Untergruppe von $\mathrm{TU}(V,f)$ auf Π zweifach transitiv operiert und folglich alle unitären Transvektionen enthält. Also ist sie gleich $\mathrm{TU}(V,f)$. Hieraus folgt, dass die (2×2)-Matrizen, die Abbildungen aus $TU(V,f)$ bezüglich der Basis b_1, b_2 darstellen,

nur Koeffizienten aus $Z(K)$ haben. Daher ist auch $r \in Z(K)$. Damit ist gezeigt, dass

$$N = \mathrm{TU}(V,f) \cap Z\bigl(\mathrm{GL}(V)\bigr) \subseteq Z\bigl(\mathrm{TU}(V,f)\bigr)$$

ist.

Es sei $\zeta \in Z(\mathrm{TU}(V,f))$ und aK sei ein isotroper Punkt. Dann wird durch $v^\tau := v - af(a,v)$ eine unitäre Transvektion definiert. Es folgt

$$v - af(a,v) = v^\tau = v^{\zeta^{-1}\tau\zeta} = v - a^\zeta f(a, v^{\zeta^{-1}}).$$

Hieraus folgt die Existenz eines $k \in K^*$ mit $a^\zeta = ak$. Daher ist

$$\zeta \in T\mathrm{U}(V,f) \cap Z\bigl(\mathrm{GL}(V)\bigr),$$

so dass $Z(T\mathrm{U}(V,f)) = N$ ist. Damit ist der Satz in allen seinen Teilen bewiesen.

8.12. Satz. *Es sei K ein Körper, dessen Zentrum von* $\mathrm{GF}(2)$, $\mathrm{GF}(3)$, $\mathrm{GF}(4)$ *und* $\mathrm{GF}(9)$ *verschieden sei. Es sei f eine nicht ausgeartete, antisymmetrische, spurwertige α-Form auf dem K-Vektorraum V. Ferner sei* $\mathrm{Rg}_K(V) \geq 2$ *und der Index von f sei mindestens* 1 *und* Π *sei die Menge der isotropen Punkte von V. Ist dann N der Normalteiler von* $\mathrm{TU}(V,f)$, *der aus allen Abbildungen von* $\mathrm{TU}(V,f)$ *besteht, die alle Punkte von* Π *in sich abbilden, ist ferner M ein Normalteiler von* $\mathrm{TU}(V,f)$, *der nicht in N enthalten ist, so ist* $M = \mathrm{TU}(V,f)$. *Insbesondere ist die Gruppe*

$$\mathrm{PTU}(V,f) := \mathrm{TU}(V,f)/N$$

einfach.

Beweis. Weil der Index von f mindestens gleich 1 ist, gibt es eine nicht isotrope Gerade H, die mindestens zwei isotrope Punkte trägt. Es sei U die Untergruppe von $\mathrm{TU}(V,f)$ die von den Transvektionen von $\mathrm{TU}(V,f)$ erzeugt wird, deren Zentren auf H liegen. Jedes Element von U lässt $H^\perp$ vektorweise fest. Wie der Beweis von Satz 8.8 zeigt — hier benutzen wir die Voraussetzungen über das Zentrum von K —, ist jede Transvektion aus U ein Kommutator in U, so dass $U = U'$ ist. Dies werden wir zweimal benutzen.

Es sei U^* die Gruppe, die von U auf der Menge der auf H liegenden Punkte induziert wird. Ist dann f^* die Einschränkung von f auf H, so folgt mit 8.11, dass U^* zu $\mathrm{PTU}(G,f^*)$ isomorph ist. Diese Gruppe operiert auf der Menge der isotropen Punkte von H zweifach transitiv, also insbesondere primitiv, wie wir wissen. Außerdem ist U^* perfekt, da U perfekt ist. Da der Stabilisator eines isotropen Punktes von H in U^* den abelschen Normalteiler enthält, der von den Transvektionen mit diesem Punkt als Zentrum induziert wird, und da diese Normalteiler die Gruppen U^* erzeugen, ist U^* nach dem Satz III.2.1 von Iwasawa einfach.

Es sei M ein Normalteiler von U, der nicht im Zentrum von U enthalten ist. Ferner sei Z das Zentrum von U. Dann operieren die Elemente von Z als Skalarmultiplikationen auf H und als Identität auf $H^\perp$. Daher operiert die

Einschränkung von M auf die Menge der Punkte von H nicht trivial. Weil U^* einfach ist, ist also $M^* = U^*$. Es folgt $MZ = U$. Weiter folgt

$$U/M = (MZ)/M \cong Z/(M \cap Z),$$

so dass U/M abelsch ist. Hieraus folgt $U = U' \subseteq M$ und damit $U = M$. — Diesem Argument sind wir in Kapitel III schon einmal begegnet.

Es sei nun M ein Normalteiler von $\mathrm{TU}(V, f)$, der nicht im Zentrum von $\mathrm{TU}(V, f)$ enthalten ist. Nach Satz 8.8 gibt es dann einen isotropen Punkt P und ein $\sigma \in N$ mit $P \neq P^\sigma$. Wir zeigen, dass es sogar einen isotropen Punkt Q gibt mit $Q^\sigma \not\leq Q^\perp$. Dazu dürfen wir annehmen, dass $P \leq P^\sigma$ ist. Es sei $P = vK$. Dann ist also $f(v, v^\sigma) = 0$. Wegen $P \neq P^\sigma$ ist

$$P^\perp \neq (P^\sigma)^\perp.$$

Es gibt also ein $z \in (P^\sigma)^\perp - P^\perp$. Setze $H := zK + P$. Wegen $P \leq P^\perp$ und $zK \cap P^\perp = \{0\}$ folgt

$$\begin{aligned} H \cap H^\perp &= (zK + P) \cap P^\perp \cap (zK)^\perp \\ &= \big((zK \cap P^\perp) + P\big) \cap (zK)^\perp \\ &= P \cap (zK)^\perp. \end{aligned}$$

Aus $zK \cap P^\perp = \{0\}$ folgt auch $(zK)^\perp + P = V$. Da $(zK)^\perp$ eine Hyperebene ist, folgt schließlich $(zK)^\perp \cap P = \{0\}$. Also ist $H \cap H^\perp = \{0\}$, so dass H nicht isotrop ist. Daher gibt es neben P noch zwei weitere isotrope Punkte yK und $y'K$ auf H. Es gibt ferner eine Transvektion τ mit Zentrum $y'K$, die vK auf yK abbildet. Es gibt also ein $l \in K$ mit $v^\sigma = yl$.

Es gibt $a, b \in K$ mit $y' = va + zb$. Es folgt

$$f(y', v^\sigma) = f(va + zb, v^\sigma) = a^\alpha f(v, v^\sigma) + b^\alpha f(z, v^\sigma) = 0,$$

da ja $f(v, v^\sigma) = 0 = f(z, v^\sigma)$ ist. Dies zeigt, dass v^σ in der Achse $(y'K)^\perp$ von τ liegt. Daher ist $v^{\sigma\tau} = v^\sigma$. Es folgt

$$v^{\sigma\tau^{-1}\sigma^{-1}\tau} = v^{\sigma\sigma^{-1}\tau} = v^\tau = yl.$$

Nun ist aber $\sigma(\tau^{-1}\sigma^{-1}\tau) \in N$ und $f(v, yl) \neq 0$. Letzteres, weil $H = vK + yK$ ist und weil H nicht isotrop ist. Damit ist gezeigt, dass es eine Abbildung in G gibt, die wir wieder σ nennen, so dass $P^\sigma \not\leq P^\perp$ gilt.

Es sei τ eine von 1_V verschiedene Transvektion mit dem Zentrum P. Dann ist $\sigma^{-1}\tau\sigma$ eine Transvektion mit dem Zentrum P^σ. Wegen $P \neq P^\sigma$ und $P \not\leq (P^\sigma)^\perp$ sind τ und $\sigma^{-1}\tau\sigma$ nicht vertauschbar. Dann sind auch τ^{-1} und $\sigma^{-1}\tau$ nicht vertauschbar. Daher ist

$$\tau^{-1}\sigma^{-1}\tau\sigma$$

ein Element der Gruppe U, die von den Elationen mit einem Zentrum auf H erzeugt wird, welches nicht im Zentrum von U liegt. Also ist $M \cap U$ ein Normalteiler von U, der nicht im Zentrum von U liegt. Nach der Eingangs gemachten Bemerkung ist folglich

$$U = M \cap U \subseteq M.$$

Daher enthält M alle Transvektionen mit dem Zentrum P und wegen der Transitivität von $\mathrm{TU}(V,f)$ auf der Menge aller isotropen Punkte überhaupt alle unitären Transvektionen. Folglich ist $M = \mathrm{TU}(V,f)$. Hieraus folgt wiederum, dass $\mathrm{PTU}(V,f)$ einfach ist.

Wie schon gesagt, gibt es nicht kommutative Körper, deren Zentren zu $\mathrm{GF}(2)$, $\mathrm{GF}(3)$, $\mathrm{GF}(4)$ oder $\mathrm{GF}(9)$ isomorph sind. Ob es auch solche gibt, die einen involutorischen Antiautomorphismus besitzen, weiß ich nicht. Wenn ja, so ist die $\mathrm{PTU}(V,f)$ auch in diesen Fällen einfach, wie Dieudonné zeigte. Wir werden dies hier aber nicht weiter verfolgen. Ist K kommutativ, so kommen die Fälle $\mathrm{GF}(2)$ und $\mathrm{GF}(3)$ nicht vor, da diese beiden Körper keinen involutorischen Antiautomorphismus besitzen. Es bleiben also nur noch die unitären Gruppen über $\mathrm{GF}(4)$ und $\mathrm{GF}(9)$ zu untersuchen. Dies werden wir in einem etwas allgemeineren Rahmen im übernächsten Abschnitt tun.

9. Endliche unitäre Gruppen

Unser erstes Ziel in diesem Abschnitt ist, die Ordnung der endlichen unitären Gruppen zu bestimmen. Anschließend werden wir die Geometrie der vollständig isotropen Unterräume einer unitären Polarität eines endlichen projektiven Raumes studieren, um im letzten Abschnitt dann die Einfachheit der $\mathrm{PTU}(V,f)$ auch in den Fällen, dass der zugrunde liegende Körper $\mathrm{GF}(4)$ oder $\mathrm{GF}(9)$ ist, zu beweisen, wobei es, wie schon erwähnt, drei Ausnahmen gibt, von denen wir zwei bereits kennen und die dritte in diesem Abschnitt kennen lernen werden.

Ist K ein kommutativer Körper und ist α ein involutorischer Automorphismus von K, so ist K eine quadratische Erweiterung des Fixkörpers von α. Ist K endlich, so ist also $K = \mathrm{GF}(q^2)$. Da die Automorphismengruppe eines endlichen Körpers zyklisch ist, hat $\mathrm{GF}(q^2)$ nur einen involutorischen Automorphismus α. Für diesen gilt $k^\alpha = k^q$ für alle $k \in K$.

9.1. Satz. *Es sei V ein Vektorraum des Ranges $n \geq 1$ über $\mathrm{GF}(q^2)$ und α sei der involutorische Automorphismus von $\mathrm{GF}(q^2)$. Ist dann f eine nicht ausgeartete symmetrische α-Form auf V, so gibt es eine Basis $b_1, \ldots, b_n$ von V mit*

$$f\bigl(\textstyle\sum_{i:=1}^n b_i k_i, \sum_{j:=1}^n b_j l_j\bigr) = \sum_{i:=1}^n k_i^\alpha l_i$$

für alle k_i, $l_j \in \mathrm{GF}(q^2)$.

Jede solche Basis heißt *Orthonormalbasis*.

Beweis. Weil f nicht ausgeartet ist, gibt es ein $v \in V$ mit $f(v,v) \neq 0$. Wegen $f(v,v) = f(v,v)^\alpha$ ist $f(v,v) \in \mathrm{GF}(q)$. Weil $f(v,v) \neq 0$ und weil die multiplikative Gruppe von $\mathrm{GF}(q^2)$ zyklisch ist, gibt es ein $k \in \mathrm{GF}(q^2)^*$ mit

$$k^{\alpha+1} = k^{q+1} = f(v,v).$$

Setze $b_1 := vk^{-1}$. Dann ist

$$f(b_1,b_1) = k^{-\alpha} f(v,v) k^{-1} = k^{-\alpha} k^{\alpha+1} k^{-1} = 1.$$

Es folgt $V = b_1K \oplus (b_1K)^\perp$. Dies impliziert wiederum, dass die Einschränkung von f auf $(b_1K)^\perp$ nicht entartet ist. Daher gibt es eine Basis $b_2, \ldots, b_n$ von $(b_1K)^\perp$ mit $f(b_i, b_i) = 1$ für $i := 2, \ldots, n$ und $f(b_i, b_j) = 0$ für $i, j := 1, \ldots, n$ und $i \neq j$. Damit ist 9.1 bewiesen.

Dieser Satz ist grundlegend für alles Folgende. Er besagt unter anderem, dass ein endlicher projektiver Raum über $\mathrm{GF}(q^2)$ im Wesentlichen nur eine unitäre Polarität besitzt. Um 9.1 ausnutzen zu können, beweisen wir zunächst

9.2. Satz. *Es sei $0 \neq k \in \mathrm{GF}(q)$. Ist $A_{n,q}$ die Anzahl der n-Tupel $y_1, \ldots, y_n$ mit $y_i \in \mathrm{GF}(q^2)$ für alle i, die die Gleichung*

$$\sum_{i:=1}^{n} y_i^{q+1} = k$$

erfüllen, so ist

$$A_{n,q} = q^{2n-1} - (-1)^n q^{n-1}.$$

Insbesondere ist $A_{n,q}$ von k unabhängig.

Beweis. Die multiplikative Gruppe von $\mathrm{GF}(q^2)$ ist zyklisch und hat die Ordnung $q^2 - 1$. Daher ist das Potenzieren mit $q + 1$ ein Epimorphismus dieser Gruppe auf die multiplikative Gruppe von $\mathrm{GF}(q)$. Der Kern dieses Epimorphismus hat die Ordnung $q + 1$. Folglich hat jedes von 0 verschiedene Element von $\mathrm{GF}(q)$ genau $q+1$ Urbilder unter diesem Epimorphismus, während die Gleichung $k^{q+1} = 0$ genau eine Lösung hat, nämlich $k = 0$.

Es sei $n > 1$. Ist $\sum_{i:=1}^{n-1} y_i^{q+1} = k$, so ist $y_n = 0$. Daher ist die Anzahl der n-Tupel dieser Art gleich

$$A_{n-1,q}.$$

Ist $\sum_{i:=1}^{n-1} y_i^{q+1} \neq k$, so gibt es nach der Eingangs gemachten Bemerkung genau $q+1$ Werte y_n mit $\sum_{i:=1}^{n} y_i^{q+1} = k$, da ja $k - \sum_{i:=1}^{n-1} y_i^{q+1} \in \mathrm{GF}(q)$ gilt. Da es von dieser Sorte $(n-1)$-Tupel genau

$$q^{2(n-1)} - A_{n-1,q}$$

Stück gibt, ist

$$A_{n,q} = A_{n-1,q} + (q+1)(q^{2(n-1)} - A_{n-1,q}) = q^{2n-1} + q^{2(n-1)} - qA_{n-1,q}.$$

Es sei nun $n = 1$. Nach der eingangs gemachten Bemerkung hat die Gleichung $y_1^{q+1} = k$ genau $q + 1$ Lösungen, so dass der Satz in diesem Falle korrekt ist. Es sei $n > 1$ und der Satz gelte für $n - 1$. Dann ist

$$A_{n,q} = q^{2n-1} + q^{2(n-1)} - q\big(q^{2n-3} - (-1)^{n-1}q^{n-2}\big) = q^{2n-1} - (-1)^n q^{n-1},$$

q. e. d.

Es sei K ein Körper und α sei ein involutorischer Antiautomorphismus von K. Ferner sei V ein K-Vektorraum und f sei eine nicht ausgeartete, spurwertige,

symmetrische α-Form auf V. Wir setzen $\mathrm{SU}(V,f) := U \cap \mathrm{SL}(V)$ und bezeichnen mit $\mathrm{PGU}(V,f)$ und $\mathrm{PSU}(V,f)$ die von $\mathrm{U}(V,f)$ bzw. $\mathrm{SU}(V,f)$ auf $\mathrm{L}(V)$ induzierten Kollineationsgruppen. Weil $\mathrm{SL}(V)$ alle Transvektionen enthält, gilt

$$\mathrm{TU}(V,f) \subseteq \mathrm{SU}(V,f)$$

und dann auch $\mathrm{PTU}(V,f) \subseteq \mathrm{PSU}(V,f)$. Gleichheit gilt sicher dann nicht, wenn der Index von f Null ist. Sie gilt aber auch im Falle, dass der Index mindestens 1 ist nicht immer. Ist K kommutativ, so gibt es aber nur eine Ausnahme, wie wir noch sehen werden.

Ist $K = \mathrm{GF}(q^2)$, so gibt es nach Satz 9.1 bis auf Isometrie nur eine unitäre Polarität. Daher bezeichnen wir in diesem Falle die Gruppen $\mathrm{U}(V,f)$ etc. auch mit $\mathrm{U}(n,q^2)$ etc., wenn n der Rang von V ist.

9.3. Satz. *Es sei n eine natürliche Zahl und q sei Potenz einer Primzahl p. Dann gilt:*

a) *Es ist*

$$\left|\mathrm{U}(n,q^2)\right| = \prod_{i:=1}^{n} \big(q^i - (-1)^i\big) q^{i-1}.$$

b) *Es ist*

$$\left|\mathrm{SU}(n,q^2)\right| = \prod_{i:=2}^{n} \big(q^i - (-1)^i\big) q^{i-1}.$$

c) *Es ist*

$$\left|\mathrm{PGU}(n,q^2)\right| = \prod_{i:=2}^{n} \big(q^i - (-1)^i\big) q^{i-1}.$$

d) *Es sei $n \geq 2$. Dann ist*

$$\left|\mathrm{PSU}(n,q^2)\right| = \frac{1}{\mathrm{ggT}(n,q+1)} \prod_{i:=2}^{n} \big(q^i - (-1)^i\big) q^{i-1}.$$

Die Ordnung einer p-Sylowgruppe irgendeiner dieser Gruppen ist $q^{\frac{1}{2}n(n-1)}$.

Beweis. a) Es sei V ein Vektorraum des Ranges n über $\mathrm{GF}(q^2)$, es sei α der involutorische Automorphismus von $\mathrm{GF}(q^2)$ und f sei eine nicht ausgeartete, symmetrische α-Form auf V. Ferner sei $b_1, \ldots, b_n$ eine nach 9.1 existierende Orthonormalbasis. Ist dann $v = \sum_{i:=1}^n b_i k_i$, so ist genau dann $f(v,v) = 1$, wenn $\sum_{i:=1}^n k^{q+1} = 1$ ist. Mit 9.2 folgt, dass

$$A_{n,q} = \big(q^n - (-1)^n\big) q^{n-1}$$

die Anzahl dieser Vektoren ist. Aufgrund des Satzes von Witt (Satz 7.2) ist $\mathrm{U}(n,q^2)$ auf der Menge der Vektoren der Länge 1 transitiv. Daher ist

$$\left|\mathrm{U}(n,q^2)\right| = A_{n,q} \left|\mathrm{U}(n,q^2)_v\right|,$$

wenn v ein Vektor der Länge 1 ist. Die Gruppe $\mathrm{U}(n,q^2)_v$ operiert treu auf $(v\mathrm{GF}(q^2))^\perp$, weil sie den Punkt $v\mathrm{GF}(q^2)$ vektorweise festlässt und weil $V = v\mathrm{GF}(q^2) \oplus (v\mathrm{GF}(q^2))^\perp$. Da die Einschränkung von f auf $(v\mathrm{GF}(q^2))^\perp$ nicht ausgeartet ist, induziert $\mathrm{U}(n,q^2)_v$ auf $(v\mathrm{GF}(q^2))^\perp$ eine Untergruppe von $\mathrm{U}(n-1,q^2)$, die wegen des Satzes von Witt sogar gleich $\mathrm{U}(n-1,q^2)$ ist. Daher ist

$$\big|\mathrm{U}(n,q^2)\big| = A_{n,q}\big|\mathrm{U}(n-1,q^2)\big|.$$

Hieraus folgt mit Induktion die Aussage a).

b) Es sei $\sigma \in \mathrm{U}(n,q^2)$. Ferner sei a die Matrix, die σ bezüglich der Orthonormalbasis $b_1, \ldots, b_n$ darstellt. Aus $f(b_i^\sigma, b_j^\sigma) = f(b_i, b_j)$ folgt dann, dass

$$(a^{-1})_{ij} = a_{ji}^q$$

ist. Hieraus folgt weiter, dass

$$1 = \det(a)^{q+1}$$

ist. Ist andererseits $k \in \mathrm{GF}(q^2)$, gilt $k^{q+1} = 1$ und definiert man σ durch $b_1^\sigma := b_1 k$ und $b_i^\sigma := b_i$ für $i \geq 2$, so ist $\sigma \in \mathrm{U}(n,q^2)$ und es gilt $\det(\sigma) = k$. Also ist det ein Epimorphismus von $\mathrm{U}(n,q^2)$ auf die Gruppe

$$\big\{k \mid k \in \mathrm{GF}(q^2), k^{q+1} = 1\big\}.$$

Da diese Gruppe die Ordnung $q+1$ hat und $\mathrm{SU}(n,q^2)$ der Kern von det ist, gilt auch b).

c) Für $n = 1$ ist nichts zu beweisen. Es sei also $n \geq 2$. Induziert dann $\delta \in \mathrm{U}(n,q^2)$ auf $\mathrm{L}(V)$ die Identität, so gibt es ein $k \in \mathrm{GF}(q^2)$ mit $v^\delta = vk$. Es folgt $k^{q+1} = 1$. Umgekehrt definiert jedes solche k ein $\delta \in \mathrm{U}(n,q^2)$, welches auf $\mathrm{L}(V)$ die Identität induziert. Weil es genau $q+1$ solcher k gibt, gilt auch c).

d) Es sei $\delta \in \mathrm{SU}(n,q^2)$ und δ induziere auf $\mathrm{L}(V)$ die Identität. Dann ist einmal $v^\delta = vk$ mit einem $k \in \mathrm{GF}(q^2)$, für das $k^{q+1} = 1$ gilt. Andererseits ist $1 = \det(\delta) = k^n$. Folglich ist $k^{\mathrm{ggT}(n,q+1)} = 1$. Gilt umgekehrt diese Gleichung und definiert man δ durch $v^\delta := vk$, so ist $\delta \in \mathrm{SU}(n,q^2)$ und δ induziert die Identität in $\mathrm{L}(V)$. Also gilt auch d).

Die letzte Aussage ist banal. Damit ist alles bewiesen.

9.4. Satz. *Es sei V ein Vektorraum des Ranges $n \geq 2$ über $\mathrm{GF}(q^2)$ und α sei der involutorische Automorphismus von $\mathrm{GF}(q^2)$. Ist f eine nicht entartete, symmetrische α-Form auf V und bezeichnet $T_{n,q}^1$ die Anzahl der bezüglich f isotropen Punkte von $\mathrm{L}(V)$, so gilt:*
a) *Es ist $T_{n,q}^1 = T_{n-1,q}^1 + A_{n-1,q}$, wobei A die in Satz 9.2 definierte Matrix ist.*
b) *Es ist*

$$T_{n,q}^1 = \frac{1}{q^2-1}(q^n - (-1)^n)(q^{n-1} - (-1)^{n-1}).$$

Beweis. a) Nach 9.1 gibt es eine Basis $b_1, \ldots, b_n$ mit

$$f\big(\textstyle\sum_{i:=1}^n b_i x_i, \sum_{j:=1}^n b_j y_j\big) = \sum_{i:=1}^n x_i^q y_i.$$

Es sei
$$P = \left(\sum_{i:=1}^n b_i x_i\right)\mathrm{GF}(q^2)$$
ein Punkt von V. Genau dann ist P isotrop, wenn
$$\sum_{i:=1}^n x_i^{q+1} = 0$$
ist. Die Punkte mit $x_n = 0$ füllen eine nicht isotrope Hyperebene H. Weil H nicht isotrop ist, ist $T^1_{n-1,q}$ die Anzahl der auf H liegenden isotropen Punkte bezüglich f.

Es sei P ein isotroper Punkt, der nicht auf H liegt. Dann ist $x_n \neq 0$. Wir setzen $y_i := x_i x_n^{-1}$. Dann ist
$$P = (b_1 y_1 + \ldots + b_{n-1} y_{n-1} + b_n)\mathrm{GF}(q^2).$$
Es folgt
$$\sum_{i:=1}^{n-1} y_i^{q+1} = -1.$$
Umgekehrt definiert jedes $(n-1)$-Tupel y, welches diese Gleichung erfüllt, einen isotropen Punkt und verschiedene solche $(n-1)$-Tupel definieren verschiedene Punkte. Mit 9.2 folgt daher, dass $A_{n-1,q}$ die Anzahl der bezüglich f isotropen Punkte ist, die nicht auf H liegen. Damit ist a) bewiesen.

b) Weil f eine unitäre Polarität darstellt und unitäre Polaritäten nach Satz 1.9 sich auch durch schiefsymmetrische α-Semibilinearformen darstellen lassen, folgt aus Satz 8.3, dass $T^1_{2,q} = q + 1$ ist. Daher gilt b) für $n = 2$. Der Rest folgt mit einer einfachen Induktion unter Zuhilfenahme von a).

Ist V ein Vektorraum des Ranges n über $\mathrm{GF}(q^2)$, ist α der involutorische Automorphismus von $\mathrm{GF}(q^2)$ und ist f eine nicht ausgeartete, symmetrische α-Semibilinearform auf V, so bezeichnen wir mit $T^r_{n,q}$ die Anzahl der bezüglich f vollständig isotropen Teilräume des Ranges r von V. Auf Grund von Satz 9.1 ist $T^r_{n,q}$ nicht von der Wahl von f abhängig. Mittels der Bemerkung nach 6.3 folgt $T^r_{n,q} = 0$, falls $r > \frac{n}{2}$ ist.

9.5. Satz. *Es sei V ein Vektorraum des Ranges $n \geq 2$ über $\mathrm{GF}(q^2)$ und α sei der involutorische Automorphismus dieses Körpers. Ist dann f eine nicht ausgeartete symmetrische α-Form auf V, so gilt für die Anzahlen der bezüglich f vollständig isotropen Teilräume:*
a) *Ist $1 \leq s \leq r \leq \frac{n}{2}$, so ist*
$$T^s_{n,q} T^{r-s}_{n-2s,q} = T^r_{n,q} \binom{r}{s, q^2}.$$
b) *Ist $1 \leq r \leq \frac{n}{2}$, so ist*
$$T^r_{n,q} = \frac{\prod_{i:=n+1-2r}^n (q^i - (-1)^i)}{\prod_{j:=1}^r (q^{2j} - 1)}.$$

Beweis. a) Wir betrachten die folgende Inzidenzstruktur: die Punkte sind die vollständig isotropen Unterräume des Ranges s und die Blöcke sind die vollständig isotropen Unterräume des Ranges r, wobei die Inzidenz mit der in $\mathrm{L}(V)$ gegebenen Relation $\leq$ identisch sei. Dann ist $T^s_{n,q}$ die Anzahl der Punkte und $T^r_{n,q}$ die Anzahl der Blöcke dieser Inzidenzstruktur. Ferner ist $\binom{r}{s,q^2}$ die Anzahl der Punkte pro Block, da ja jeder Teilraum eines vollständig isotropen Teilraums vollständig isotrop ist. Ist U ein vollständig isotroper Teilraum des Ranges s, so induziert f wegen $\perp^2 = 1_{\mathrm{L}(V)}$ auf $U^\perp/U$ eine nicht ausgeartete symmetrische α-Semibilinearform. Ferner gilt, dass jeder vollständig isotrope Teilraum, der U umfasst, in $U^\perp$ enthalten ist. Hieraus folgt, dass die Anzahl der vollständig isotropen Teilräume des Ranges r von V, die U umfassen, gleich der Anzahl der vollständig isotropen Teilräume des Ranges $r-s$ von $U^\perp/U$, dh. gleich $T^{r-s}_{n-2s,q}$ ist. Mit IIII.1.2c) folgt nun die Behauptung.

b) Mit $s = 1$ folgt aus a) mit I.7.6 und 9.3b)

$$\begin{aligned}\frac{q^{2r}-1}{q^2-1}T^r_{n,q} &= \binom{r}{1,q^2}T^r_{n,q} = T^1_{n,q}T^{r-1}_{n-2,q}\\ &= \frac{1}{q^2-1}(q^n-(-1)^n)(q^{n-1}-(-1)^{n-1})T^{r-1}_{n-2,q}.\end{aligned}$$

Hieraus folgt per Induktion die Behauptung.

Ist $n = 3$, so gibt es auf Grund der Bemerkung nach 6.3 keine vollständig isotropen Geraden. Dies macht die Menge der isotropen Punkte in diesem Falle besonders homogen und damit besonders interessant. Diese Sonderrolle der projektiven Ebenen werden wir nun — vom Hauptweg unserer Untersuchungen abweichend — etwas eingehender betrachten. Dabei spielt die Endlichkeit nur bei den Anzahlbestimmungen eine Rolle.

Es sei K ein Körper und α sei ein involutorischer Antiautomorphismus von K. Ferner sei V ein Vektorraum des Ranges 3 über K und f sei eine nicht ausgeartete, symmetrische α-Semibilinearform auf V, deren Index mindestens 1 sei. Wie wir wissen, ist die letzte Bedingung überflüssig, da automatisch erfüllt, wenn K endlich ist. Mit $\mathrm{Un}(V,f)$ bezeichnen wir die Geometrie aus den bezüglich f isotropen Punkten und den nicht isotropen Geraden, die wenigstens einen isotropen Punkt tragen. Man nennt $\mathrm{Un}(V,f)$ *Unital*.

9.6. Satz. *Es sei K ein Körper und α sei ein involutorischer Antiautomorphismus von K. Ferner sei V ein Vektorraum des Ranges* 3 *über K und f sei eine nicht ausgeartete, symmetrische, spurwertige α-Form auf V, deren Index* 1 *sei. Dann gilt:*

a) *Durch zwei verschiedene Punkte von* $\mathrm{Un}(V,f)$ *geht genau eine Gerade von* $\mathrm{Un}(V,f)$.

b) *Ist P ein Punkt von* $\mathrm{Un}(V,f)$ *und ist G eine von $G^\perp$ verschiedene Gerade durch P, so ist G eine Gerade von* $\mathrm{Un}(V,f)$.

c) *Ist K endlich, also* $K = \mathrm{GF}(q^2)$, *so ist* $\mathrm{Un}(V,f)$ *ein* 2-$(q^3+1,q+1,1)$ *Blockplan.*

d) *Die Gruppe* $\mathrm{PGU}(V,f)$ *operiert zweifach transitiv auf der Menge der Punkte von* $\mathrm{Un}(V,f)$.

Beweis. a) Es seien P und Q zwei verschiedene Punkte von $\mathrm{Un}(V, f)$. Weil $\perp$ eine Polarität ist, folgt mit Satz II.4.1, dass $P + Q$ keine absolute Gerade ist. Da es keine vollständig isotropen Geraden gibt, ist $P + Q$ also nicht isotrop und folglich eine Gerade von $\mathrm{Un}(V, f)$. Durch zwei verschiedene Punkte von $\mathrm{Un}(V, f)$ geht also mindestens und damit genau eine Gerade von $\mathrm{Un}(V, f)$.

b) Nach dem zu II.4.1 dualen Satz ist $P^\perp$ die einzige absolute Gerade durch P. Folglich ist G nicht isotrop und damit eine Gerade von $\mathrm{Un}(V, f)$.

c) Dies folgt mit a) und Satz 9.3 b).

d) Ist G eine Gerade von $\mathrm{Un}(V, f)$, so gibt es einen und nach Satz 8.3 dann mindestens drei isotrope Punkte auf G. Dann gibt es aber eine Basis a, b von G mit isotropen Vektoren a und b, so dass $f(a, b) = 1$ ist. Dies zeigt, dass alle Geraden von $\mathrm{Un}(V, f)$ isometrisch sind. Mit dem Satz von Witt (Satz 7.2) folgt daher, dass $\mathrm{PGU}(V, f)$ auf der Menge der Geraden von $\mathrm{Un}(V, f)$ transitiv operiert. Ist G wieder eine Gerade von $\mathrm{Un}(V, f)$, so haben wir früher schon gesehen, dass die Gruppe, die von allen Transvektionen mit Zentren auf G erzeugt wird, auf der Menge der Punkte von G zweifach transitiv operiert. Mit a) folgt daher auch die letzte Behauptung.

Ist $K = \mathrm{GF}(q^2)$, so ist $\mathrm{Un}(V, f)$ also ein 2-$(q^3 + 1, q + 1, 1)$ Blockplan. Mit b) etwa folgt, dass die Anzahl der Geraden von $\mathrm{Un}(V, f)$ durch eine Punkt dieser Geometrie gleich q^2 ist. Es folgt, dass die Anzahl der Geraden von $\mathrm{Un}(V, f)$ gleich $q^2(q^2 - q + 1)$ ist. Also trägt jede Gerade von $\mathrm{L}(V)$ einen Punkt von $\mathrm{Un}(V, f)$.

Ist V ein Vektorraum des Ranges 3 über $\mathrm{GF}(4)$, ist α der involutorische Automorphismus von $\mathrm{GF}(4)$ und ist f eine nicht entartete, symmetrische α-Form auf V, so ist $\mathrm{Un}(V, f)$ nach Satz 9.5c) ein 2-$(9, 3, 1)$ Blockplan, so dass $\mathrm{Un}(V, f)$ nichts anderes ist als eine affine Ebene der Ordnung 3. Diese Situation, nämlich die Einbettung der affinen Ebene der Ordnung 3 in eine projektive Ebene, haben wir in Abschnitt III.7 ausführlich studiert. Es steht zu erwarten, dass die hessesche Gruppe im vorliegenden Falle als die Gruppe $\mathrm{PGU}(V, f)$ zu interpretieren ist. Dies ist tatsächlich der Fall, wie wir uns nun überlegen werden.

Dazu sei P ein Punkt von $\mathrm{L}(V)$. Ist P ein Punkt von $\mathrm{Un}(V, f)$, so ist $P^\perp$ die einzige Gerade durch P, die mit $\mathrm{Un}(V, f)$ nur den Punkt P gemeinsam hat, wie 9.5b) sagt. Ist P kein Punkt von $\mathrm{Un}(V, f)$, so ist $P \not\leq P^\perp$. Daher ist $P^\perp$ eine Gerade von $\mathrm{Un}(V, f)$. Ist Q ein Punkt von $\mathrm{Un}(V, f)$, der auf $P^\perp$ liegt, so ist $Q^\perp = P + Q$. Es gibt also drei Geraden durch P, die $\mathrm{Un}(V, f)$ in genau einem Punkt treffen und diese drei Punkte sind kollinear. Die restlichen zwei Geraden durch P sind nicht isotrop und sind daher Geraden von $\mathrm{Un}(V, f)$. Diese beiden Geraden und die Gerade $P^\perp$ sind die drei Geraden einer Parallelenschar der affinen Ebene $\mathrm{Un}(V, f)$. Dies zeigt, dass $\perp$ vollständig durch die Einbettung von $\mathrm{Un}(V, f)$ in $\mathrm{L}(V)$ beschrieben wird. Daher ist die hessesche Gruppe im Zentralisator von $\perp$ enthalten. Da die hessesche Gruppe der Stabilisator von $\mathrm{L}(V)$ in $\mathrm{PGL}(V)$ ist, ist sie sogar gleich $\mathrm{PGU}(V, f)$. Nach III.7.8 enthält die hessesche Gruppe den Normalteiler T der Translationen der affinen Ebene $\mathrm{Un}(V, f)$. Ist σ eine Elation ungleich 1 aus $\mathrm{PGU}(V, f)$, so enthält die Gruppe $T\{1, \sigma\}$ alle Ela-

tionen aus $\mathrm{PGU}(V,f)$, da T auf der Menge der Punkte von $\mathrm{Un}(V,f)$ transitiv ist. Also ist

$$\mathrm{PTU}(V,f) = T\{1,\sigma\}.$$

Somit ist $\mathrm{PTU}(V,f)$ auch in diesem Falle nicht einfach. Überdies gilt hier

$$\left|\mathrm{PTU}(V,f)\right| = 9 \cdot 2 \neq 9 \cdot 8 = \left|\mathrm{PSU}(V,f)\right|,$$

so dass $\mathrm{PTU}(V,f) \neq \mathrm{PSU}(V,f)$ ist.

9.7. Satz. *Es sei V ein Vektorraum des Ranges $n \geq 2$ über $\mathrm{GF}(q^2)$ und α sei der involutorische Automorphismus von $\mathrm{GF}(q^2)$. Ferner sei f eine nicht entartete, symmetrische α-Form auf V. Ist P ein isotroper Punkt, so bezeichnen wir mit $O(P)$ die Menge der von P verschiedenen, zu P orthogonalen und mit $N(P)$ die Menge der zu P nicht orthogonalen isotropen Punkte von V. Dann ist*

$$\left|O(P)\right| = q^2 T^1_{n-2,q} \qquad \textit{und} \qquad \left|N(P)\right| = q^{2n-3}.$$

Beweis. Es ist $O(P)$ die Menge der von P verschiedenen isotropen Punkte auf $P^\perp$. Ist $Q \in O(P)$, so ist $P, Q \leq Q^\perp$ und $P, Q \leq P^\perp$. Also ist

$$P + Q \leq P^\perp \cap Q^\perp = (P+Q)^\perp.$$

Folglich ist $P+Q$ vollständig isotrop. Ist andererseits G eine vollständig isotrope Gerade durch P, so ist $G \leq P^\perp$ und alle von P verschiedenen Punkte auf G gehören zu $O(P)$. Da die vollständig isotropen Geraden durch P den isotropen Punkten von $P^\perp/P$ entsprechen, gilt also

$$\left|O(P)\right| = q^2 T^1_{n-2,q}.$$

Hieraus folgt mit 9.5 weiter, dass die Anzahl der Punkte in $N(P)$ gleich

$$T^1_{n,q} - q^2 T^1_{n-2,q} - 1 = q^{2n-3}$$

ist.

9.8. Satz. *Es sei V ein Vektorraum des Ranges $n \geq 2$ über dem kommutativen Körper K und α sei ein involutorischer Automorphismus von K. Ferner sei f eine nicht entartete, symmetrische, spurwertige α-Form auf V, deren Index mindestens 1 sei. Ist P ein isotroper Punkt, so bezeichnen wir mit $O(P)$ die Menge der von P verschiedenen, zu P orthogonalen und mit $N(P)$ die Menge der zu P nicht orthogonalen isotropen Punkte von V. Dann sind die Mengen $O(P)$ und $N(P)$ Bahnen von $\mathrm{PSU}(V,f)_P$.*

Beweis. Ist $n = 2$, so ist $O(P) = \emptyset$ und die Gruppe $\mathrm{PTU}(V,f)$ ist auf der Menge der isotropen Punkte von $\mathrm{L}(V)$ zweifach transitiv, wie wir schon verschiedentlich bemerkten. Daher ist $N(P)$ eine Bahn von $\mathrm{PTU}(V,f)_P$ und damit auch von $\mathrm{PSU}(V,f)_P$. Wir dürfen daher annehmen, dass $n \geq 3$ ist.

Zunächst beachten wir jedoch, unabhängig vom Rang und vom Index, dass V eine Orthogonalbasis hat. Es gibt ja sicherlich ein $b_1 \in V$ mit $f(b_1, b_1) \neq 0$.

Dann ist $(b_1K)^\perp$ nicht isotrop. Nach Induktionsannahme gibt es daher eine Orthogonalbasis $b_2, \ldots, b_n$ von $(b_1K)^\perp$, so dass $b_1, b_2, \ldots, b_n$ eine Orthogonalbasis von V ist.

Es sei $\sigma \in U(V,f)$ und es gelte $b_j = \sum_{i:=1}^n b_i a_{ij}$. Definiere ferner die Matrix c durch $c_{ij} := f(b_i, b_j)$. Dann ist

$$c = (a^\alpha)^t ca.$$

Wegen $\det(c) = \prod_{i:=1}^n f(b_i, b_i) \neq 0$ ist daher

$$\det(\sigma)^{\alpha+1} = \det(a)^{\alpha+1} = 1.$$

Entsprechend interpretiert gilt dieser Sachverhalt auch bei nicht kommutativem K.

Zurück zum Beweise des Satzes. Wir zeigen zunächst, dass $N(P)$ eine Bahn von $\mathrm{PSU}(V,f)_P$ ist. Dazu seien Q, $R \in N(P)$. Es gibt dann ein $q \in Q$ und ein $r \in R$ mit

$$f(p,q) = f(p,r) = 1.$$

Weil auch

$$f(q,q) = f(r,r) = 0$$

gilt, gibt es nach dem Satz von Witt ein $\tau \in \mathrm{U}(V,f)$ mit $p^\tau = p$ und $q^\tau = r$. Wir setzen $G := P + Q$. Dann ist G eine nicht isotrope Gerade, so dass $V = G \oplus G^\perp$ ist. Es gibt einen nicht isotropen Vektor $s \in G^\perp$. Setze $k := \det(\tau)$. Nach unserer zuvor gemachten Bemerkung ist $k^{\alpha+1} = 1$ und daher auch $k^{-\alpha-1} = 1$. Definiere σ durch $s^\sigma := sk^{-1}$ und $u^\sigma = u$ für alle $u \in (sK)^\perp$. Es folgt $\sigma \in \mathrm{U}(V,f)$, da K kommutativ ist. Wegen p, $r \in (sK)^\perp$ folgt $p^{\tau\sigma} = p$ und $q^{\tau\sigma} = r$, so dass $P^{\tau\sigma} = P$ und $Q^{\tau\sigma} = R$ ist. Schließlich ist $\det(\tau\sigma) = 1$, so dass $\tau\sigma \in \mathrm{SU}(V,f)$ gilt. Dies zeigt, dass $N(P)$ eine Bahn von $\mathrm{PSU}(V,f)_P$ ist, da $N(P)$ ja unter $\mathrm{PSU}(V,f)_P$ invariant ist.

Nun zeigen wir, dass auch $O(P)$ eine Bahn von $\mathrm{PSU}(V,f)_P$ ist. Da es gleichgültig ist, mit welcher Form $\perp$ dargestellt wird, nehmen wir für den Augenblick an, dass f schiefsymmetrisch sei. Sind x, x', y, $y' \in P^\perp$ und gilt $x - x'$, $y - y' \in P$, so ist $f(x,y) = f(x', y')$, wie man leicht nachrechnet. Daher wird durch $f(x+P, y+P) := f(x,y)$ eine schiefsymmetrische, ebenfalls nicht ausgeartete α-Form auf $P^\perp/P$ definiert. Ist $q + P$ ein isotroper Vektor von $P^\perp/P$, ist $l \in K$ und gilt $l^\alpha = l$, so wird durch

$$(v+P)^\tau := v + P + (q+P)lf(q+P, v+P)$$

eine unitäre Transvektion auf $P^\perp/P$ definiert. Wegen

$$(v+P)^\tau = v + qlf(q,v) + P$$

wird τ von einer Transvektion aus $\mathrm{PSU}(V,f)_P$ induziert. Weil die isotropen Punkte von $P^\perp/P$ den vollständig isotropen Geraden durch P entsprechen, folgt mittels 8.4, dass $\mathrm{PSU}(V,f)_P$ auf der Menge der vollständig isotropen Geraden durch P transitiv operiert.

Es sei f wieder die ursprüngliche Form. Sind nun Q, $R \in O(P)$, so gibt es also ein $\gamma \in \mathrm{PSU}(V,f)_P$ mit $Q^\gamma \leq P + R$. Wir dürfen also des weiteren annehmen, dass $P+Q = P+R$ ist. Die Gerade $P+Q$ ist vollständig isotrop. Nach 6.3 gibt es eine vollständig isotrope Gerade G, so dass $(P+Q) \cap G = \{0\}$ ist und $P+Q+G$ nicht isotrop ist. Setze $U := P+Q+G$. Dann ist also U ein nicht isotroper Raum des Ranges 4. Die Einschränkung von f auf U ist nicht ausgeartet und definiert eine Polarität, die wir mit $\perp(U)$ bezeichnen. Wegen $\mathrm{Rg}_K(U) = 4$ ist $P+Q = (P+Q)^{\perp(U)}$ und $G = G^{\perp(U)}$.

Setze $T := Q^{\perp(U)} \cap G$. Dann ist T ein Punkt auf G. Es folgt

$$P^{\perp(U)} \cap T = P^{\perp(U)} \cap Q^{\perp(U)} \cap G = (P+Q)^{\perp(U)} \cap G = (P+Q) \cap G = \{0\}.$$

Somit ist $P^{\perp(U)} \cap G$ ein von T verschiedener Punkt auf G. Es gibt noch einen Punkt S auf G, der von T und $P^{\perp(U)} \cap G$ verschieden ist. Es sei $T = tK$. Dann ist $f(q,t) = 0$. Wegen $T \not\leq P^{\perp(U)}$ gibt es ein $p \in P$ mit $f(p,t) = 1$. Ebenso gibt es ein $s \in S$ mit $f(p,s) = 1$. Wegen $S \neq T$ gibt es schließlich ein $q \in Q$ mit $f(q,s) = 1$. Es sei $R = rK$. Es gibt dann ein $\lambda \in K$ mit $r = q + p\lambda$. Definiert man σ durch

$$\begin{aligned} p^\sigma &:= p \\ q^\sigma &:= p\lambda + q \\ s^\sigma &:= s(1-\lambda^\alpha) + t\lambda^\alpha \\ t^\sigma &:= -s\lambda^\alpha + t(1+\lambda^\alpha) \end{aligned}$$

und $u^\sigma := u$ für alle $u \in (P+Q+G)^\perp$, so zeigt eine einfache Rechnung, dass $\sigma \in U(V,f)$ und $\det(\sigma) = 1$ ist. Also ist $\sigma \in \mathrm{SU}(V,f)_P$ und es gilt $Q^\sigma = R$. Damit ist alles bewiesen, da auch $O(P)$ unter $\mathrm{PSU}(V,f)_P$ invariant ist.

9.9. Satz. *Es sei K ein kommutativer Körper und α sei ein involutorischer Automorphismus von K. Ist V ein K-Vektorraum des Ranges $n \geq 2$ und ist f eine nicht entartete, symmetrische und spurwertige α-Form auf V, deren Index mindestens* 1 *ist, so operiert die Gruppe* $\mathrm{PSU}(V,f)$ *auf der Menge der isotropen Punkte primitiv.*

Beweis. Ist der Index von f gleich 1, so ist $N(P) = \emptyset$ für alle isotropen Punkte P von $\mathrm{L}(V)$. In diesem Falle ist $\mathrm{PSU}(V,f)$ nach 9.8 auf der Menge der isotropen Punkte zweifach transitiv, also erst recht primitiv.

Wir nehmen nun an, der Satz sei falsch. Dann ist der Index von f mindestens 2 und folglich $n \geq 4$. Es sei Δ ein Imprimitivitätsgebiet von $\mathrm{PSU}(V,f)$. Ist $P \in \Delta$, so gibt es noch einen weiteren Punkt in Δ, so dass mit 9.8 folgt, dass $\Delta = \{P\} \cup O(P)$ oder $\Delta = \{P\} \cup N(P)$ ist.

1. Fall: Es sei $\Delta = \{P\} \cup O(P)$. Wegen $n \geq 4$ ist der Rang von $P^\perp/P$ mindestens 2. Weil f auf $P^\perp/P$ eine nicht entartete Form induziert, gibt es eine Ebene E mit $P \leq E \leq P^\perp$, so dass E/P eine Gerade von $P^\perp/P$ ist, die mindestens zwei isotrope Punkte enthält. Ist dann G ein Komplement von P in E, so folgt aus $E \leq P^\perp$, dass E/P und G isometrisch sind. Es gibt daher zwei isotrope Vektoren v, $w \in G$ mit $f(v,w) = 1$. Es gilt

$$vK,\ wK \in O(P) \subseteq \Delta,$$

und daher
$$\{vK\} \cup O(vK) = \Delta = \{wK\} \cup O(wK).$$
Wegen $vK \neq wK$ ist daher $wK \in O(vK)$, so dass wir den Widerspruch $0 = f(v,w) = 1$ erhalten.

2. Fall: Es sei $\Delta = \{P\} \cup N(P)$. Es sei $P = vK$. Weil der Index von f mindestens 2 ist, gibt es eine vollständig isotrope Gerade G und in jedem Falle auch eine nicht isotrope Gerade H durch P (Satz 8.10). Es gibt dann einen isotropen Vektor $u \in H$ mit $f(v,u) = 1$. Es sei $w \in G - P$. Es ist $uK \in N(P) \subseteq \Delta$. Also ist
$$\Delta = \{uK\} \cup N(uK).$$
Setze $s := v + w$. Dann ist $P \neq sK$. Außerdem ist $f(v,s) = f(v,v) + f(v,w) = 0$. Also ist $sK \in O(P)$ und damit
$$sK \notin \Delta.$$
Andererseits ist $f(u,s) = f(u,v) + f(u,u) = 1$ und daher
$$sK \in N(uK) \subseteq \Delta,$$
so dass wir auch in diesem Falle einen Widerspruch erhalten. Damit ist der Satz bewiesen.

Wir beschließen diesen Abschnitt, indem wir einen weiteren Ausnahmeisomorphismus etablieren.

9.10. Satz. *Die Gruppen* $\mathrm{PSU}(4,4)$ *und* $\mathrm{PSp}(4,3)$ *sind isomorph.*

Beweis. Es sei V ein Vektorraum des Ranges 4 über $\mathrm{GF}(4)$ und f sei eine nicht ausgeartete α-Form auf V, wobei α der involutorische Automorphismus von $\mathrm{GF}(4)$ sei. Wir definieren eine Inzidenzstruktur $\Delta = (\Pi, \mathrm{B}, \mathrm{I})$ wie folgt: ist P ein Punkt von $\mathrm{L}(V)$, so gehöre P genau dann zu Π, wenn P nicht isotrop ist. Ferner sei $\mathrm{B} := \{P^\perp \mid P \in \Pi\}$. Es gelte $Q \ \mathrm{I}\ P^\perp$ genau dann, wenn $Q = P$ oder wenn $Q \leq P^\perp$ ist.

Die Anzahl der Punkte von $\mathrm{L}(V)$ ist $4^3 + 4^2 + 4 + 1 = 85$. Nach 9.4b) ist die Anzahl der isotropen Punkte gleich $(4+1)i \cdot 9 = 45$. Daher ist die Anzahl v der Punkte von Δ gleich 40. Dann ist aber auch $|\mathrm{B}| = 40$, da $\perp$ ja bijektiv ist. Ist $P \in \Pi$, so ist die Anzahl aller Punkte von $P^\perp$ gleich $4^2 + 4 + 1 = 21$. Daher inzidieren in Δ mit $P^\perp$ genau $21 - 9 + 1 = 13$ Punkte. Ebenso sieht man, dass jedes $P \in \Pi$ in Δ mit genau 13 Blöcken inzidiert. Also ist Δ eine taktische Konfiguration mit den Parametern $v = b = 40$ und $k = r = 13$.

Es seien P und Q zwei verschiedene Punkte von Δ.

1. Fall: Es ist $P \leq Q^\perp$. Dann ist auch $Q \leq P^\perp$. Mittels des Modulargesetzes folgt
$$\begin{aligned}(P+Q) \cap (P+Q)^\perp &= (P+Q) \cap P^\perp \cap Q^\perp \\ &= \big((P \cap P^\perp) + Q\big) \cap Q^\perp = Q \cap Q^\perp = \{0\}.\end{aligned}$$

Somit ist $P+Q$ nicht isotrop, trägt also genau drei isotrope und dann genau zwei nicht isotrope Punkte, nämlich P und Q. Dann trägt aber auch die Gerade $(P+Q)^\perp$ genau zwei nicht isotrope Punkte, die wir P_1 und Q_1 nennen. Es folgt, dass P und Q simultan mit genau den Blöcken $P^\perp$, $Q^\perp$, $P_1^\perp$, $Q_1^\perp$ inzidieren. Auf all diesen Blöcken liegen aber auch die Punkte P_1 und Q_1, so dass die Δ-Gerade durch P und Q genau vier Punkte enthält.

2. Fall: Es ist $P \not\leq Q^\perp$. Dann ist auch $Q \not\leq P^\perp$. Weil alle nicht isotropen Geraden isometrisch sind, kann $P+Q$ nicht nicht isotrop sein. Daher gibt es auf $P+Q$ genau einen isotropen Punkt, nämlich $\mathrm{rad}(P+Q)$ und neben P und Q noch zwei weitere nicht isotrope Punkte R und S. Weil $P+Q$ und $(P+Q)^\perp$ symmetrische Rollen spielen, gibt es auf $(P+Q)^\perp$ ebenfalls vier nicht isotrope Punkte P_1, Q_1, R_1 und S_1. Die Punkte P und Q inzidieren in Δ simultan also mit genau den Blöcken $P_1^\perp$, $Q_1^\perp$, $R_1^\perp$, $S_1^\perp$. Darüber hinaus liegen auch R und S auf der Δ-Geraden durch P und Q.

Damit ist gezeigt, dass Δ ein 2-$(40,13,4)$ Blockplan ist, dessen Geraden alle

$$4 = \frac{40-4}{13-4} = \frac{b-\lambda}{r-\lambda}$$

Punkte tragen. Nach IIII.10.1 besteht Δ also aus den Punkten und Hyperebenen einer projektiven Geometrie, da ja auch $v-k = 40-13 \geq 2$ ist. Diese Geometrie hat die Ordnung $q=3$ und dann wegen

$$40 = 1+3+3^2+3^3$$

— einer Zerlegung der 40, die schon bei Fibonacci eine Rolle spielte — den Rang 4. Also ist Δ zur Geometrie der Punkte und Ebenen eines Vektorraums vom Rang 4 über $\mathrm{GF}(3)$ isomorph. Die Abbildung π, die durch $P^\pi := P^\perp$ und $(P^\perp)^\pi := P$ definiert wird, ist offenbar eine Polarität von Δ, die von einer symplektischen Polarität der zugehörigen projektiven Geometrie herrührt. Es folgt $\mathrm{PGU}(4,4) \subseteq \mathrm{PSp}(4,3)$. Nach 9.3 ist

$$\bigl|\mathrm{PSU}(4,4)\bigr| = \bigl|\mathrm{PGU}(4,4)\bigr| = 2^6 \cdot 3 \cdot 9 \cdot 15$$

und nach 3.3 ist

$$\bigl|\mathrm{PSp}(4,3)\bigr| = \frac{1}{2} \cdot 3^4 \cdot 8 \cdot 80 = 2^6 \cdot 3 \cdot 9 \cdot 15.$$

Also ist $\mathrm{PSU}(4,4) = \mathrm{PSp}(4,3)$, q. e. d.

9.11. Korollar. *Die Gruppe* $\mathrm{PSU}(4,4)$ *ist einfach.*

Beweis. Dies folgt mit 9.10 aus 3.11.

10. Die speziellen unitären Gruppen

Unser nächstes Ziel ist zu zeigen, dass bis auf eine Ausnahme, die wir schon kennen, $\mathrm{TU}(V,f) = \mathrm{SU}(V,f)$ gilt, falls der V zugrunde liegende Körper kommutativ ist. Dies werden wir dann benutzen, um die Einfachheit der $\mathrm{PSU}(V,f)$ in den noch fehlenden Fällen nachzuweisen.

10.1. Satz. *Es sei K ein Körper und α sei ein involutorischer Antiautomorphismus von K. Ist V ein Vektorraum des Ranges $n \geq 2$ über K und ist f eine nicht entartete, symmetrische, spurwertige α-Form auf V, deren Index mindestens gleich 1 ist, so gibt es zu jedem $v \in V$ eine nicht isotrope, isotrope Punkte tragende Gerade G mit $v \in G$.*

Beweis. Ist $f(v,v) = 0$, so folgt dies mit 8.10. Es sei also $f(v,v) \neq 0$. Weil f spurwertig ist, gibt es ein $b \in K$ mit $f(v,v) = b + b^\alpha$. Weil der Index von f mindestens 1 ist, gibt es eine Gerade $H = v_1K + v_2K$ mit isotropen v_i, so dass $f(v_1, v_2) = 1$ ist. Es folgt

$$f(v_1 + v_2b, v_1 + v_2b) = b^\alpha + b = f(v,v).$$

Nach dem Satz von Witt gibt es ein $\sigma \in \mathrm{U}(V,f)$ mit $(v_1 + b_2b)^\sigma = v$. Setze $G := H^\sigma$. Dann ist G eine Gerade der verlangten Art.

10.2. Satz. *Es sei K ein kommutativer Körper, der mehr als 4 Elemente enthalte, und α sei ein involutorischer Automorphismus von K. Ferner sei V ein Vektorraum des Ranges $n \geq 3$ über K und f sei eine nicht ausgeartete, symmetrische, spurwertige α-Form auf V, deren Index mindestens 1 sei. Sind v_1, $v_2 \in V$, gilt $f(v_1,v_1) = f(v_2,v_2) \neq 0$, ist $v_1K \neq v_2K$ und ist die Gerade $v_1K + v_2K$ isotrop, so gibt es ein $v_3 \in V$ mit $f(v_3,v_3) = f(v_1,v_1)$, so dass $v_1K + v_3K$ und $v_2K + v_3K$ nicht isotrope Geraden sind.*

Beweis. Setze $G := v_1K + v_2K$. Weil $f(v_1,v_1) \neq 0$ ist, ist

$$G = v_1K \oplus \mathrm{rad}(G),$$

wobei $\mathrm{rad}(U) := U \cap U^\perp$ für alle $U \in \mathrm{L}(V)$ gesetzt sei. Es gibt einen Vektor $r \in \mathrm{rad}(G)$ und ein $a \in K$ mit

$$v_2 = r + v_1a.$$

Es folgt

$$f(v_1,v_1) = f(v_2,v_2) = a^\alpha f(v_1,v_1)a.$$

Weil $f(v_1,v_1) \neq 0$ und weil K kommutativ ist, folgt

$$1 = a^{\alpha+1}.$$

Wegen $v_2 \notin v_1K$ ist $r \neq 0$. Ferner ist $r \in (v_1K)^\perp$. Weil $(v_1K)^\perp$ nicht isotrop ist, gibt es einen weiteren isotropen Vektor $r' \in (v_1K)^\perp$ mit $f(r,r') = 1$.

Setze $L := \{k \mid k \in K, k^\alpha = k\}$. Dann ist L ein Teilkörper von K mit $[K : L] = 2$. Es folgt, dass L mindestens drei Elemente enthält, da K mehr als vier Elemente enthält. Die Norm der Erweiterung $K : L$ ist bekanntlich die durch $N(k) := k^{1+\alpha}$ definierte Abbildung N. Die Menge $N(K^*)$ enthält alle Quadrate von L und und damit mindestens ein von 1 verschiedenes Element, falls L mehr als drei Elemente enthält. Dies ist aber auch richtig, falls $|L| = 3$ ist, da in diesem Falle $N(K^*) = L$ ist. Es gibt also ein $z \in K^*$ mit $N(z) \neq 1$.

Ist $k \in K - L$, so ist $k^{1-\alpha} \neq 1$. Ferner gilt $N(k^{1-\alpha}) = 1$. Folglich ist $\mathrm{Kern}(N)$ nicht trivial. Weil andererseits auch $N(K^*)$ mindestens zwei Elemente

enthält, enthält $N(K^*)$ zunächst mindestens ein, dann aber mindestens zwei Elemente, die von $f(v_1, v_1)$ verschieden sind. Es gibt daher ein $t \in N(K^*)$ mit $t \neq f(v_1, v_1)$, $a^\alpha z f(v_1, v_1)$. Wegen $t \in N(K^*)$ ist $t^\alpha = t$, was wir noch benutzen werden.

Setze $y := t - a^\alpha z f(v_1, v_1)$. Dann ist $y \neq 0$.

Weil f spurwertig ist, gibt es ein $k \in K$ mit

$$k + k^\alpha = -zz^\alpha f(v_1, v_1) + f(v_1, v_1).$$

Setze $x := y^{-\alpha} k$. Dann ist

$$xy^\alpha + x^\alpha y = -zz^\alpha f(v_1, v_1) + f(v_1, v_1).$$

Setze nun $v_3 := rx + r'y + v_1 z$. Dann ist

$$f(v_3, v_3) = x^\alpha y + y^\alpha x + zz^\alpha f(v_1, v_1) = f(v_1, v_1).$$

Um nachzuweisen, dass $v_1K + v_3K$ nicht isotrop ist, genügt es nachzuweisen, dass die Determinante der Matrix

$$\begin{pmatrix} f(v_1, v_1) & f(v_1, v_3) \\ f(v_3, v_1) & f(v_3, v_3) \end{pmatrix}$$

nicht Null ist. Wegen $f(v_1, v_1) = f(v_3, v_3)$ und $f(v_1, v_3) = zf(v_1, v_1)$ ist diese Determinante gleich

$$f(v_1, v_1)^2(1 - zz^\alpha),$$

also in der Tat von Null verschieden, da ja $zz^\alpha \neq 1$ ist.

Um nachzuweisen, dass $v_2K + v_3K$ nicht isotrop ist, muss man entsprechend nachweisen, dass die Determinante der Matrix

$$\begin{pmatrix} f(v_2, v_2) & f(v_2, v_3) \\ f(v_3, v_2) & f(v_3, v_3) \end{pmatrix}$$

ungleich Null ist. Wegen

$$f(v_3, v_3) = f(v_1, v_1) = f(v_2, v_2)$$

und

$$f(v_2, v_3) = y + a^\alpha z f(v_1, v_1) = t$$

ist diese Determinante gleich

$$f(v_1, v_1)^2 - tt^\alpha = f(v_1, v_1)^2 - t^2 \neq 0.$$

Damit ist der Satz bewiesen.

10.3. Satz. *Es sei K ein kommutativer Körper und α sei ein involutorischer Automorphismus von K. Ferner sei V ein K-Vektorraum des Ranges $n \geq 3$. Ist $|K| = 4$, so sei $n \geq 4$. Ist f eine nicht ausgeartete, symmetrische, spurwertige*

α-Form auf V, deren Index mindestens 1 ist, sind v_1, $v_2 \in V$ und gilt $f(v_1, v_1) = f(v_2, v_2) \neq 0$, so gibt es ein $\gamma \in \mathrm{TU}(V, f)$ mit $v_1^\gamma = v_2$.

Beweis. Es sei zunächst $v_1 K = v_2 K$. Dann ist $v_2 = v_1 a$ mit einem $a \in K$. Es folgt $f(v_1, v_1) = a^\alpha f(v_1, v_1)a$ und daher $a^{1+\alpha} = 1$, da ja $f(v_1, v_1) \neq 0$ ist. Nach 10.1 gibt es eine nicht isotrope Gerade durch $v_1 K$, die zwei isotrope Punkte trägt. Es sei $0 \neq u \in G \cap (v_1 K)^\perp$. Weil v_1 nicht isotrop ist, ist u, v_1 eine Basis von G. Definiere nun σ durch

$$x^\sigma := \begin{cases} v_2, & \text{falls } x = v_1 \\ ua^{-\alpha}, & \text{falls } x = u \\ x, & \text{falls } x \in G^\perp. \end{cases}$$

Dann ist σ ein Element von $\mathrm{SU}(V, f)$. Die unitären Transvektionen, deren Zentren auf G liegen, erzeugen eine Untergruppe S von $\mathrm{SU}(V, f)$, die auf G die $\mathrm{SU}(G, f)$ induziert, wie aus Satz 8.9 folgt. Weil σ auf G ein Element der $\mathrm{SU}(G, f)$ induziert und auf $G^\perp$ gleich der Identität ist, folgt $\sigma \in S$, so dass $\sigma \in \mathrm{TU}(V, f)$ ist.

Es sei also $v_1 K \neq v_2 K$. Setze $G := v_1 K + v_2 K$.

1. Fall: G ist nicht isotrop, enthält aber isotrope Punkte. Hier definieren wir σ durch

$$x^\sigma := \begin{cases} v_2, & \text{falls } x = v_1 \\ -v_1, & \text{falls } x = v_2 \\ x, & \text{falls } x \in G^\perp \end{cases}$$

und schließen wie eben weiter.

2. Fall: G enthält keine isotropen Punkte. Dies hat zur Konsequenz, dass K nicht endlich ist. Dies werden wir noch auszunutzen haben.

Nach 10.1 gibt es eine nicht isotrope Gerade H durch den Punkt $(v_1 - v_2)K$, die isotrope Punkte trägt. Es ist also $V = H \oplus H^\perp$. Es gibt daher $w_i \in H$ und $s_i \in H^\perp$ mit $v_i = w_i + s_i$. Es folgt

$$s_1 - s_2 = v_1 - v_2 + w_2 - w_1 \in H \cap H^\perp = \{0\}.$$

Setzt man $s := s_1$, so ist also $v_i = w_i + s$ für $i := 1, 2$. Ferner gilt

$$f(v_1, v_1) = f(w_1, w_1) + f(s, s)$$

und

$$f(v_2, v_2) = f(w_2, w_2) + f(s, s)$$

und folglich

$$f(w_1, w_1) = f(w_2, w_2).$$

Ist $f(w_1, w_1) \neq 0$, so gibt es, wie im ersten Fall gesehen, ein $\sigma \in \mathrm{TU}(V, f)$ mit $w_1^\sigma = w_2$ und $s^\sigma = s$. Es folgt $v_1^\sigma = v_2$.

Es seien w_1 und w_2 isotrop. Weil α nicht die Identität ist, gibt es ein $a \in K$ mit $a^\alpha \neq a$. Setze $k := a - a^\alpha$. Dann ist $k \neq 0$ und $k^\alpha = -k$. Setze ferner $g := kf$. Dann ist g schiefsymmetrisch und es gilt $\mathrm{SU}(V, f) = \mathrm{SU}(V, g)$ und $\mathrm{TU}(V, f) = \mathrm{TU}(V, g)$. Ferner gilt $f(v, v) = f(w, w)$ genau dann, wenn

$g(v,v) = g(w,w)$ ist. Also dürfen wir bei den nun folgenden Betrachtungen f durch g ersetzen. Wir setzen

$$L := \{k \mid k \in K, k^\alpha = k\}.$$

Ferner setzen wir $a := g(w_1, w_2)$. Weil G keine isotropen Punkte trägt, ist $g(v_1 - v_2, v_1 - v_2) \neq 0$. Andererseits ist

$$\begin{aligned} g(v_1 - v_2, v_1 - v_2) &= g(w_1 - w_2, w_1 - w_2) \\ &= -g(w_1, w_2) - g(w_2, w_1) = -a + a^\alpha, \end{aligned}$$

so dass $a^\alpha \neq a$ ist. Somit ist $a \notin L$. Setze $w := w_1 a + w_2$. Dann ist

$$g(w,w) = a^\alpha g(w_1, w_2) + g(w_2, w_1)a = a^\alpha a - a^\alpha a = 0$$

und

$$g(v_1, w) = g(w_1 + s, w_1 a + w_2) = g(w_1, w_2) = a \neq 0$$

sowie

$$g(v_2, w) = g(w_2 + s, w_1 a + w_2) = g(w_2, w_1)a = -a^\alpha a \neq 0.$$

Für $x \in L$ setze

$$\begin{aligned} p(x) := x^2 (a^{1+\alpha})^3 + x a^{1+\alpha} \big(a^\alpha g(v_1, v_2) + a g(v_1, v_2)^\alpha\big) \\ + g(v_1, v_1)^2 + g(v_1, v_2) g(v_1, v_2)^\alpha. \end{aligned}$$

Wegen

$$\big(g(v_1, v_1)^2\big)^\alpha = \big(g(v_1, v_1)^\alpha\big)^2 = \big(-g(v_1, v_1)\big)^2 = g(v_1, v_1)^2$$

ist p eine Abbildung von L in sich.

Für $y \in L$ setze

$$q(y) := y^2 g(v_1, v_1) + y\big(g(v_1, v_2) + g(v_2, v_1)\big) + g(v_1, v_1).$$

Hat p keine Nullstelle in L, so sei η irgendein Element von L^*. Hat p eine Nullstelle in L, so hat p zwei Nullstellen ν_1 und ν_2, falls man Vielfachheiten ggf. mitzählt. Weil K unendlich ist, ist auch L unendlich. Es gibt daher ein $\eta \in L^*$ mit

$$q(\eta) + \nu_i \eta a a^\alpha (a - a^\alpha) \neq 0.$$

Setze

$$\xi := \frac{-q(\eta)}{\eta a a^\alpha (a - a^\alpha)}.$$

Dann ist $\xi \in L$, da ξ unter α invariant bleibt, wie man sich rasch überzeugt. Aus

$$q(\eta) + \xi \eta a a^\alpha (a - a^\alpha) = 0$$

folgt, dass ξ keine Nullstelle von p ist. Also ist $p(\xi) \neq 0$. Wir definieren nun τ durch

$$v^\tau := v - w \xi g(w, v).$$

Dann ist
$$v_1^\tau = v_1 - w\xi f(w, v_1) = v_1 + w\xi a^\alpha.$$
Wir zeigen, dass $v_2K + v_1^\tau K$ nicht isotrop ist, aber isotrope Punkte trägt. Eine einfache Rechnung zeigt, dass
$$\det\begin{pmatrix} g(v_2, v_2) & g(v_2, v_1^\tau) \\ g(v_1^\tau, v_2) & g(v_1^\tau, v_1^\tau) \end{pmatrix} = p(\xi) \neq 0$$
ist. Dies zeigt, dass $v_2K+v_1^\tau K$ nicht isotrop ist. Ferner gilt $v_1^\tau + v_2\eta \in v_2K+v_1^\tau K$ und
$$g(v_1^\tau + v_2\eta, v_1^\tau + v_2\eta) = q(\eta) + \eta\xi a a^\alpha(a - a^\alpha) = 0.$$
Daher ist $v_2K+v_1^\tau K$ eine isotrope Punkte tragende nicht isotrope Gerade. Nach Fall 1 gibt es daher ein $\sigma \in \mathrm{TU}(V, g)$ mit $v_1^{\tau\sigma} = v_2$. Damit ist der fragliche Sachverhalt auch in diesem Falle bewiesen.

3. Fall: G ist isotrop und K enthält mehr als vier Elemente. Nach 10.2 gibt es dann ein $v_3 \in V$ mit $g(v_1, v_1) = g(v_3, v_3)$, so dass die Geraden $v_1K + v_3K$ und $v_3K + v_2K$ nicht singulär sind. Mittels der bereits erledigten Fälle 1 und 2 gelangt man daher ans Ziel.

4. Fall: G ist isotrop und K enthält genau vier Elemente. Nach Voraussetzung ist dann $n \geq 4$. Es folgt $\mathrm{Rg}_K(G^\perp) = n - 2 \geq 2$. Wäre $G^\perp$ vollständig isotrop, so folgte
$$G^\perp \leq G^{\perp\perp} = G$$
und damit $n - 2 \leq 2$, so dass $G = G^\perp$ wäre. Somit wäre G vollständig isotrop, was nicht der Fall ist, da $g(v_1, v_1) \neq 0$ ist. Weil $G^\perp$ also nicht isotrop ist, gibt es ein $v_3 \in G^\perp$ mit $g(v_3, v_3) \neq 0$. Es folgt, dass die Geraden $v_1K + v_3K$ und $v_2K + v_3K$ nicht singulär sind, so dass auch in diesem Falle mit Fall 1 die Behauptung folgt.

10.4. Satz. *Es sei K ein kommutativer Körper und α sei ein involutorischer Automorphismus von K. Ist V ein Vektorraum des Ranges $n \geq 2$ über K und ist f eine nicht ausgeartete, symmetrische, spurwertige α-Form auf V, deren Index mindestens* 1 *sei, so ist $SU(V, f) = TU(V, f)$, es sei denn, es ist $n = 3$ und $|K| = 4$.*

Beweis. Ist $n = 2$, so folgt dies aus Satz 8.9. Dies nehmen wir als Induktionsverankerung, falls K mehr als vier Elemente hat. Hat K nur vier Elemente, so ist die Gruppe $\mathrm{PSU}(V, f)$ nach 9.11 einfach. Mit 9.3b) und d) folgt, dass die Gruppen $\mathrm{PSU}(V, f)$ und $\mathrm{SU}(V, f)$ wegen $\mathrm{ggT}(4, 2 + 1) = 1$ isomorph sind. Daher ist auch $\mathrm{SU}(V, f)$ in diesem Falle einfach. Weil $\mathrm{TU}(V, f)$ ein nicht trivialer Normalteiler von $\mathrm{SU}(V, f)$ ist, ist also $\mathrm{TU}(V, f) = \mathrm{SU}(V, f)$

Es sei nun $n \geq 3$ und K enthalte mehr als vier Elemente oder $n \geq 5$ und $|K| = 4$. Ferner $\sigma \in \mathrm{SU}(V)$ und $v \in V$ mit $f(v, v) \neq 0$. Nach 10.3 gibt es dann ein $\tau \in TU(V, f)$ mit $v^{\sigma\tau} = v$. Die Einschränkung von $\sigma\tau$ auf $(vK)^\perp$ ist nach Induktionsannahme ein Produkt von Transvektionen mit Zentrum in $(vK)^\perp$. Da diese den Punkt vK vektorweise festlassen, ist dieses Produkt auf ganz V gleich $\sigma\tau$. Daher ist $\sigma\tau \in \mathrm{TU}(V, f)$ und folglich $\sigma \in \mathrm{TU}(V, f)$. Damit ist der Satz bewiesen.

10.5. Satz. *Es sei K ein kommutativer Körper und α sei ein involutorischer Automorphismus von K. Ist V ein Vektorraum des Ranges $n \geq 2$ über K und ist f eine nicht entartete, symmetrische, spurwertige α-Form auf V, deren Index mindestens* 1 *sei, so ist* $\mathrm{SU}(V,f) = \mathrm{SU}(V,f)'$, *es sei denn es ist* $(n,|K|) = (2,4)$, $(2,9)$, $(3,4)$.

Beweis. Ist $n = 2$, so folgt dies mit den Sätzen 8.9 und III.2.7. Es sei also $n \geq 3$. Es sei τ eine unitäre Transvektion. Es gibt dann einen isotropen Vektor v_1 und ein $c \in K$ mit $c^\alpha = -c$, so dass

$$v^\tau = v - v_1 c f(v_1, v)$$

ist. Nach 8.10 gibt es einen isotropen Vektor v_3, so dass die Gerade $G := v_1K + v_3K$ nicht isotrop ist. Es ist $V = G \oplus G^\perp$ und $G^\perp \neq \{0\}$. Daher gibt es einen nicht isotropen Vektor $v_2 \in G^\perp$. Indem man v_3 gegebenenfalls durch einen Skalar abändert, kann man erreichen, dass $f(v_1,v_3) = f(v_2,v_2)$ ist. Weil T auf $(G + v_2K)^\perp$ die Identität induziert und

$$V = G \oplus v_2K \oplus (G + v_2K)^\perp$$

gilt, dürfen wir, um zu zeigen, dass τ ein Kommutator ist, annehmen, dass $n = 3$ ist. Dann ist v_1, v_2, v_3 eine Basis von V und es gilt

$$\begin{aligned} v_1^\tau &= v_1, \\ v_2^\tau &= v_2, \\ v_3^\tau &= v_3 - v_1 c. \end{aligned}$$

Für x, $y \in K$ definieren wir eine Abbildung $\rho(x,y) \in \mathrm{SL}(V)$ durch

$$\begin{aligned} v_1^{\rho(x,y)} &:= v_1, \\ v_2^{\rho(x,y)} &:= v_1 x + v_2, \\ v_3^{\rho(x,y)} &:= v_1 y - v_2 x^\alpha + v_3. \end{aligned}$$

Wir beachten zunächst, dass $\tau = \rho(0,-c)$ ist. Ferner gilt, wie einfache Rechnungen zeigen,

$$\rho(x',y')\rho(x,y) = \rho(x'+x, y'+y - x'^\alpha x).$$

Hieraus folgt

$$\rho(x,y)^{-1} = \rho(-x, -y - x x^\alpha)$$

und weiter

$$\rho(x',y')^{-1}\rho(x,y)^{-1}\rho(x',y')\rho(x,y) = \rho(0, x'x^\alpha - x x'^\alpha).$$

Als Nächstes suchen wir Bedingungen dafür, dass die Abbildung $\rho(x,y)$ zu $\mathrm{SU}(V,f)$ gehört. Sofort zu sehen ist, dass $\det(\rho(x,y)) = 1$ ist. Ferner ist

$$\begin{aligned}
f(v_1^{\rho(x,y)}, v_1^{\rho(x,y)}) &= f(v_1, v_1)\\
f(v_1^{\rho(x,y)}, v_2^{\rho(x,y)}) &= f(v_1, v_1x + v_2) = f(v_1, v_2)\\
f(v_1^{\rho(x,y)}, v_3^{\rho(x,y)}) &= f(v_1, v_1y - v_2c^\alpha + v_3) = f(v_1, v_3)\\
f(v_2^{\rho(x,y)}, v_2^{\rho(x,y)}) &= f(v_1x + v_2, v_1x + v_2) = f(v_2, v_2).
\end{aligned}$$

Weiter ist, da ja $f(v_1, v_3) = f(v_2, v_2)$ ist,

$$\begin{aligned}
f(v_2^{\rho(x,y)}, v_3^{\rho(x,y)}) &= f(v_1x + v_2, v_1y - v_2x^\alpha + v_3)\\
&= x^\alpha f(v_1, v_3) - f(v_2, v_2)x^\alpha = 0 = f(v_2, v_3).
\end{aligned}$$

Bis hierher ergeben sich also noch keine Einschränkungen dafür, dass $\rho(x,y)$ ein Element von $\mathrm{SU}(V,f)$ ist. Dies ändert sich jetzt. Es gilt nämlich

$$\begin{aligned}
f(v_3^{\rho(x,y)}, v_3^{\rho(x,y)}) &= f(v_1y - v_2x^\alpha + v_3, v_1y - v_2x^\alpha + v_3)\\
&= y^\alpha f(v_1, v_3) + xx^\alpha f(v_2, v_2) + yf(v_3, v_1)\\
&= (y + y^\alpha + xx^\alpha)f(v_2, v_2).
\end{aligned}$$

Bei dieser Rechnung ist zu beachten, dass

$$f(v_3, v_1) = f(v_1, v_3)^\alpha = f(v_2, v_2)^\alpha = f(v_2, v_2)$$

ist. Es gilt also $\rho(x,y) \in i\mathrm{SU}(V,f)$ genau dann, wenn

$$y + y^\alpha + xx^\alpha = 0$$

ist.

Wir beachten weiter: Es gibt ein $k \in K$ mit $k^\alpha + k \neq 0$ (Satz III.6.3). Ist $m \in L$, so setzen wir $l := (k^\alpha + k)^{-1}m$. Dann folgt

$$(lk)^\alpha + lk = m.$$

Somit ist die Abbildung $x \to x^\alpha + x$ surjektiv.

Es gibt ein $t \in K$ mit $t + t^\alpha \neq 0$. Setze

$$x := \frac{ct^\alpha}{t + t^\alpha}.$$

Wegen $c + c^\alpha = 0$ ist dann

$$x^\alpha - x = \frac{c^\alpha t - ct^\alpha}{t + t^\alpha} = \frac{c^\alpha t + ct - ct - ct^\alpha}{t + t^\alpha} = -c.$$

(Dies ist ein Spezialfall der additiven Form von Hilberts Satz 90.) Wie wir gerade bemerkten, gibt es ein $y \in K$ mit $y + y^\alpha + xx^\alpha = 0$. Ebenso gibt es ein $z \in K$ mit $z + z^\alpha + 1 = 0$. Dann sind $\rho(1,z)$, $\rho(x,y) \in \mathrm{SU}(V,f)$ und es gilt

$$\rho(1,z)^{-1}\rho(x,y)^{-1}\rho(1,z)\rho(x,y) = \rho(0, x^\alpha - x) = \rho(0, -c) = \tau.$$

Damit ist gezeigt, dass τ ein Kommutator ist. (Bis hierhin gilt der Beweis auch im Falle, dass $n = 3$ und $|K| = 4$ ist.) Weil $\mathrm{SU}(V, f)$ nach Satz 10.4 von seinen Transvektionen erzeugt wird, ist also $\mathrm{SU}(V, f) = \mathrm{SU}(V, f)'$, q. e. d.

10.6. Satz. *Es sei K ein kommutativer Körper und α sei ein involutorischer Automorphismus von K. Ferner sei V ein Vektorraum des Ranges $n \geq 2$ über K. Ist dann f eine nicht ausgeartete, symmetrische, spurwertige α-Form auf V, deren Index mindestens* 1 *ist, so ist* $\mathrm{PSU}(V, f)$ *einfach, es sei denn, es ist $n = 2$ und $K = \mathrm{GF}(4)$ oder $\mathrm{GF}(9)$ oder es ist $n = 3$ und $K = \mathrm{GF}(4)$.*

Beweis. Es sei Ω die Menge der isotropen Punkte. Dann operiert $\mathrm{PSU}(V, f)$ nach Satz 9.9 auf Ω primitiv. Mit 10.5 folgt $\mathrm{PSU}(V, f)' = \mathrm{PSU}(V, f)$, wenn man von den Ausnahmefällen absieht. Ist $P \in \Omega$, so bilden die unitären Elationen mit Zentrum P einen abelschen Normalteiler von $\mathrm{PSU}(V, f)_P$. Dieser Normalteiler erzeugt zusammen mit seinen Konjugierten nach 10.4 die Gruppe $\mathrm{PSU}(V, f)$. Nach dem Satz III.2.1 von Iwasawa ist $\mathrm{PSU}(V, f)$ also einfach.

Damit haben wir in allen uns interessierenden Fällen die Einfachheit von $\mathrm{PTU}(V, f)$ nachgewiesen.

Wie schon gesagt, werden wir uns zu einem späteren Zeitpunkt um die orthogonalen Gruppen kümmern.[4] Dabei wird für sie das Gleiche gelten wie für die unitären Gruppen, dass wir nämlich die Gruppen vom Index 0 nicht untersuchen werden. Ihre Struktur ist in beiden Fällen so eng mit der arithmetischen Struktur des Koordinatenkörpers verwoben, dass man tief in die Zahlentheorie eintauchen muss, will man Aussagen über ihre Struktur gewinnen.

[4] Anmerkung der Herausgeber: Das Kapitel über orthogonale Gruppen fehlt.

VI.

Segresche Mannigfaltigkeiten

Seit meiner Komputeralgebrazeit liebe ich freie Konstruktionen. Ich definiere daher das Tensorprodukt zweier Moduln hier in der Allgemeinheit, in der es gemeinhin in der Algebra benötigt wird, dh., allgemeiner als wir es brauchen werden, da man in dieser allgemeineren Situation nicht umhin kommt, sich freier Konstruktionen zu bedienen. Hat man dann Tensorprodukte so allgemein definiert, wie wir es tun werden, so stellt man fest, dass diese Allgemeinheit der Geometrie wiederum zugute kommt. Man kann nämlich Tensorprodukte gut dazu benutzen, Homomorphismen projektiver Verbände zu beschreiben. Darauf werden wir im zweiten Abschnitt dieses Kapitels eingehen. Dies ist das Extra, das dieses Kapitel birgt. Sein eigentliches Thema sind die Segreschen Mannigfaltigkeiten, von denen man in Büchern über projektive Geometrie auch nur selten etwas erfährt.

Investieren wir zunächst in weiteres Werkzeug.

1. Tensorprodukte

Es sei R ein Ring mit Eins. Ferner sei M ein unitärer R-Rechtsmodul und N ein unitärer R-Linksmodul. (Das Wort „unitär" werden wir uns im folgenden schenken). Es sei weiterhin A eine abelsche Gruppe, deren Verknüpfung wir als Addition notieren. Die Abbildung f von $M \times N$ in A heiße genau dann *tensoriell*, wenn gilt:
a) Es ist $f(m + m', n) = f(m, n) + f(m', n)$ für alle m, $m' \in M, n \in N$.
b) Es ist $f(m, n + n') = f(m, n) + f(m, n')$ für alle $m \in M$ und alle $n, n' \in N$.
c) Es ist $f(mr, n) = f(m, rn)$ für alle $m \in M$, für alle $n \in N$ und alle $r \in R$.
Wie es so häufig geschieht, erscheint von A nur die Verknüpfung explizit in dieser Definition.

Zu den bisherigen Daten nehmen wir noch eine abelsche Gruppe T hinzu sowie eine tensorielle Abbildung τ von $M \times N$ in T. Das Paar (T, τ) heiße ein *Tensorprodukt* von M mit N, falls gilt:
1) Ist A eine abelsche Gruppe und ist f eine tensorielle Abbildung von $M \times N$ in A, so gibt es einen Homomorphismus φ von T in A mit $f = \varphi\tau$.
2) Die Gruppe T wird von der Menge $\{\tau(m, n) \mid m \in M,\ n \in N\}$ erzeugt.

Wer sich mit universellen Objekten auskennt, wird sich über die nächsten beiden Sätze nicht wundern.

1.1. Satz. *Es sei R ein Ring mit Eins. Ferner sei M ein R-Rechtsmodul und N ein R-Linksmodul. Schließlich sei (T, τ) ein Tensorprodukt von M mit N.*

Ist A eine abelsche Gruppe und ist f eine tensorielle Abbildung von $M \times N$ in A, so gibt es genau einen Homomorphismus φ von T in A mit $f = \varphi\tau$.

Beweis. Dass es ein solches φ gibt, besagt die Definition des Tensorproduktes. Es sei ψ ein zweiter Homomorphismus mit $f = \psi\tau$. Ist dann $(m, n) \in M \times N$, so ist

$$\varphi(\tau(m, n)) = f(m, n) = \psi(\tau(m, n)).$$

Dies zeigt, dass φ und ψ auf einem Erzeugendensystem von A übereinstimmen, so dass, wie behauptet, $\psi = \varphi$ ist.

1.2. Satz. *Es sei R ein Ring mit Eins. Ferner sei M ein R-Linksmodul und N ein R-Rechtsmodul. Sind (T, τ) und (T', τ') Tensorprodukte von M mit N, so sind (T, τ) und (T', τ') isomorph.*

Beweis. Nach Voraussetzung gibt es einen Homomorphismus φ von T in T' mit $\tau' = \varphi\tau$ und einen Homomorphismus φ' von T' in T mit $\tau = \varphi'\tau'$. Hieraus folgt

$$\tau' = \varphi\varphi'\tau'.$$

Nach 1.1 ist daher $\varphi\varphi' = 1_{T'}$. Ebenso folgt, dass $\tau'\tau = 1_T$ ist. Daher ist φ ein Isomorphismus von T auf T' mit $\tau' = \varphi\tau$, so dass alles bewiesen ist.

Alle bisherigen Anstrengungen wären umsonst, gäbe es keine Tensorprodukte. Doch der mit freien Konstruktionen Vertraute weiß natürlich, wie er vorzugehen hat, um die Existenz des Tensorproduktes sicherzustellen. Wir nehmen an, dass der Leser zumindest weiß, wie man sich freie abelsche Gruppen verschafft. Wer keine Kenntnis der grundlegenden Konstruktionen freier Objekte hat, sei für diese auf mein Buch „Tools and Fundamental Constructions of Combinatorial Mathematics“ verwiesen.

1.3. Satz. *Es sei R ein Ring mit Eins. Ferner sei M ein Rechts- und N ein Linksmodul über R. Schließlich sei F die freie abelsche Gruppe über dem freien Erzeugendensystem $M \times N$ und T sei die von allen Elementen der Form*

$$(m + m', n) - (m; n) - (m', n)$$

bzw.

$$(m, n + n') - (m, n) - (m, n')$$

bzw.

$$(mr, n) - (m, rn)$$

erzeugte Untergruppe von F. Setzt man

$$M \otimes_R N := F/T$$

und definiert man τ durch

$$\tau(m, n) := (m, n) + T,$$

so ist $(M \otimes_R N, \tau)$ ein Tensorprodukt von M mit N.

Beweis. Aus der Definition von T folgt, dass τ eine tensorielle Abbildung von $M \times N$ in $M \otimes_R N$ ist. Weil $M \times N$ ein Erzeugendensystem von F ist, wird $M \otimes_R N$ von der Menge der $\tau(m,n)$ erzeugt. Es bleibt zu zeigen, dass jede tensorielle Abbildung von $M \times N$ in eine abelsche Gruppe sich durch τ faktorisieren lässt. Dies ist aber auch banal. Jede faktorielle Abbildung f von $M \times N$ in eine abelsche Gruppe A ist insbesondere eine Abbildung jener Menge in A, so dass f sich zu einem Homomorphismus g von F in A fortsetzen lässt. Weil f tensoriell ist, liegt T im Kern von g, so dass mit bekannten Sätzen folgt, dass es einen Homomorphismus φ von $F/T = M \otimes_R N$ in A gibt mit $f(m,n) = g(m,n) = (\varphi\tau)(m,n)$ für alle $(m,n) \in M \times N$. Also ist $f = \varphi\tau$, was noch zu beweisen war.

Es ist üblich, das Bild von (m,n) unter τ mit $m \otimes n$ zu bezeichnen. Dieser Konvention werden wir uns im folgenden anschließen.

Der nächste Satz ist ebenfalls von großer Bedeutung.

1.4. Satz. *Es sei R ein Ring mit Eins. Ferner seien M und M' zwei Rechts- und N und N' zwei Linksmoduln über R. Ist dann f ein Homomorphismus von M in M' und g ein Homomorphismus von N in N', so gibt es genau einen Homomorphismus, den wir mit $f \otimes g$ bezeichnen, von $M \otimes_R N$ in $M' \otimes_R N'$ mit*

$$(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$$

für alle $(m,n) \in M \times N$.

Beweis. Die durch $\sigma(m,n) := f(m) \otimes g(n)$ definierte Abbildung σ ist tensoriell, so dass die Existenz von $f \otimes g$ aus der Definition des Tensorproduktes und die Einzigkeit aus Satz 1.1 folgt.

Hat man drei R-Rechtsmoduln M, M' und M'' sowie drei R-Linksmoduln N, N' und N'', ist f ein Homomorphismus von M in M' und f' ein solcher von M' in M'', ist ferner g ein Homomorphismus und f' ein solcher von M' in M'', ist ferner g ein Homomorphismus von N in N' und g' ein Homomorphismus von N' in N'', so ist

$$(f' \otimes g')(f \otimes g) = (f'f) \otimes (g'g),$$

wie unschwer zu sehen ist.

Wie nützlich Satz 1.4 ist, sieht man schon beim Beweise des nächsten Satzes.

1.5. Satz. *Es sei R ein Ring mit Eins und M sei ein R-Rechts- und N ein R-Linksmodul. Ferner sei $(D_i \mid i \in I)$ eine Familie von Teilmoduln von M und es gelte*

$$M = \bigoplus_{i \in I} D_i.$$

Für $i \in I$ sei π_i die Projektion von M auf D_i mit $D_j \subseteq \mathrm{Kern}(\pi_i)$ für alle $j \in \mathrm{I} - \{i\}$. Setzt man $\Delta_i := (\pi_i \otimes 1)(M \otimes_R N)$ und bezeichnet man mit $\otimes_i$ die Einschränkung von $D_i \times N$, so gilt

$$M \otimes_R N = \bigoplus_{i \in I} \Delta_i$$

und $(\Delta_i, \otimes_i)$ *ist für alle* $i \in I$ *ein Tensorprodukt von* D_i *mit* N.

Beweis. Es sei $(m,n) \in M \times N$. Es gibt dann eine endliche Teilmenge J von I mit $m \in \sum_{j \in J} D_j$, dh., es ist

$$m = \sum_{j \in J} m_j$$

mit $m_j \in D_j$. Weil nach Konstruktion $\pi_i^2 = \pi_i$ für alle i und $\pi_i \pi_j = 0$ für alle i und j mit $i \neq j$ gilt, folgt $m_j = \pi_j(m)$ für alle $j \in J$ und damit

$$m = \sum_{j \in J} \pi_j(m).$$

Hiermit folgt

$$m \otimes n = \sum_{j \in J} (\pi_j(m) \otimes n) = \sum_{j \in J} (\pi_j \otimes 1)(m \otimes n),$$

so dass $m \otimes n \in \sum_{i \in I} \Delta_i$ ist. Weil $M \otimes_R N$ von der Menge der $m \otimes n$ erzeugt wird, folgt

$$M \otimes_R N = \sum_{i \in I} \Delta_i.$$

Es ist

$$(\pi_i \otimes 1)(\pi_j \otimes 1) = (\pi_i \pi_j) \otimes 1,$$

so dass die $\pi_i \otimes 1$ paarweise orthogonale Idempotente sind. Hieraus folgt, dass sogar

$$M \otimes_R N = \bigoplus_{i \in I} \Delta_i$$

gilt.

Es bleibt zu zeigen, dass $(\Delta_i, \otimes_i)$ ein Tensorprodukt von D_i mit N ist. Dazu sei f eine tensorielle Abbildung von $D_i \times N$ in eine abelsche Gruppe A. Wir definieren dann eine Abbildung F von $M \times N$ in A durch

$$F(m,n) := f(\pi_i(m), n).$$

Offenbar ist auch F tensoriell. Es gibt also einen Homomorphismus φ von $M \otimes_R N$ in A mit $F(m,n) = \varphi(m \otimes n)$. Setze $\psi := \varphi(\pi_i \otimes 1)$. Ist dann $(y,n) \in D_i \times N$, so gilt

$$\begin{aligned} f(y,n) &= F(y,n) = \varphi(y \otimes n) \\ &= \varphi(\pi_i(y) \otimes n) = \varphi((\pi_i \otimes 1)(y \otimes n)) \\ &= \psi(y \otimes_i n). \end{aligned}$$

Schließlich ist klar, dass Δ_i von der Menge der $y \otimes_i n$ erzeugt wird. Damit ist alles bewiesen.

Dieser Satz findet sich in der Literatur meist wie folgt formuliert: Unter den gemachten Voraussetzungen gilt

$$M \otimes_R N \cong \bigoplus_{i \in I} (D_i \otimes N).$$

Dies ist zwar richtig — und wir werden ihn auch wohl immer in dieser Formulierung benutzen —, doch ist dies viel weniger aussagekräftig als obige Formulierung.

Wir möchten Tensorprodukte von Vektorräumen studieren und dabei erreichen, dass die betrachteten Tensorprodukte ebenfalls Vektorräume sind. Um dorthin zu gelangen, definieren wir zunächst den Begriff des (R, S)-Bimoduls. Es seien R und S Ringe mit Eins. Die abelsche Gruppe heiße genau dann (R, S)-*Bimodul*, falls M ein R-Links- und ein S-Rechtsmodul ist und darüber hinaus $r(ms) = (rm)s$ für alle $r \in R$, alle $m \in M$ und alle $s \in S$ gilt.

1.6. Satz. *Es seien R und S zwei Ringe mit Eins. Ferner sei M ein R-Rechtsmodul und N ein (R, S) Bimodul. Dann trägt $M \otimes_R N$ genau eine S-Rechtsmodulstruktur mit $(m \times n)s = m \times ns$ für alle $m \in M$, alle $n \in N$ und alle $s \in S$.*

Beweis. Die Einzigkeit folgt wieder daraus, dass die Gesamtheit der $m \otimes n$ das Tensorprodukt $M \otimes_R N$ erzeugen.

Es sei $s \in S$. Wir definieren die Abbildung f, von $M \otimes N$ in $M \otimes_R N$ durch

$$f_s(m, n) := m \otimes ns.$$

Banale Rechnungen zeigen, dass f_s tensoriell ist. Es gibt also einen Endomorphismus φ_s von $M \otimes_R N$ mit

$$\varphi_s(m \otimes n) = m \otimes ns$$

für alle $(m, n) \in M \times N$. Definiert man nun ys für $y \in M \otimes_R N$ durch $ys := \varphi_s(y)$, so zeigen Routinerechnungen, dass $M \otimes_R N$ auf diese Weise zu einem S-Rechtsmodul wird, für den überdies $(m \otimes n)s = m \otimes ns$ für alle $m \in M$, alle $n \in N$ und alle $s \in S$ gilt.

Jeder Ring R ist natürlich ein (R, R)-Bimodul. Also trägt $M \otimes_R R$ gemäß dem gerade bewiesenen Satz eine Struktur als R-Rechtsmodul, falls M ein R-Rechtsmodul ist. Über diesen Modul gilt der folgende Satz.

1.7. Satz. *Es sei R ein Ring mit Eins und M sei ein R-Rechtsmodul. Es gibt dann einen Isomorphismus σ des R-Rechtsmoduls $M \otimes_R R$ auf M mit $\sigma(m \otimes r) = mr$ für alle $m \in M$ und alle $r \in R$.*

Beweis. Die Abbildung, die (m, r) auf mr abbildet, ist tensoriell. Es gibt daher einen Homomorphismus σ der abelschen Gruppe $M \otimes_R R$ in R mit $\sigma(m \otimes r) = mr$. Hieraus folgt unmittelbar, dass σ sogar ein Modulhomomorphismus ist. Es bleibt zu zeigen, dass σ bijektiv ist.

Ist $m \in M$, so sei $\tau(m)$ durch $\tau(m) := m \otimes 1$ gegeben. Die Abbildung τ ist sicherlich additiv. Wegen

$$\tau(mr) = mr \otimes 1 = m \otimes r = (m \otimes 1)r$$

ist τ ein Modulhomomorphismus. Nun ist aber

$$\sigma\tau(m) = m1 = m$$

und

$$\tau\sigma(m, r) = mr \otimes 1 = m \otimes r.$$

Hieraus folgt, dass σ bijektiv und dass τ die zu σ inverse Abbildung ist.

Für diesen Satz braucht man zum ersten Male, dass R eine Eins hat. Zuvor war diese Annahme immer überflüssig.

Es sei R ein Ring mit Eins und M sei ein Rechts- und N ein Linksmodul über R. Ist D ein direkter Summand von M, so zeigt Satz 1.5, dass $M \otimes_R N$ einen zu $D \otimes_R N$ einen zu $D \otimes_R N$ isomorphen direkten Summanden besitzt. Ist D nur ein Teilmodul von M, so kann man nicht schließen, dass $D \otimes_R N$ zu einem Teilmodul von $M \otimes_R N$ isomorph ist. Um dies zu belegen, sei Z der Ring der ganzen Zahlen, Z_2 die zyklische Gruppe der Ordnung 2 und Q der Körper der rationalen Zahlen. Nach Satz 1.7 ist dann *mutatis mutandis*

$$Z \otimes_Z Z_2 \cong Z_2.$$

Andererseits ist

$$Q \otimes_Z Z_2 = \{0\},$$

wie wir jetzt zeigen werden. Ist nämlich $z \in Z_2$ und $r \in Q$, so folgt

$$r \otimes z = \frac{r}{2} \otimes 2z = 0$$

und damit die Behauptung.

In Satz 1.6 haben wir gesehen, wie man aus dem Tensorprodukt $M \otimes_R N$ einen S-Rechtsmodul macht, wenn N ein (R, S)-Bimodul ist. Ganz analog sieht man, dass $M \otimes_R N$ genau eine S-Linksmodulstruktur mit

$$s(m \otimes n) = sm \otimes n$$

für alle fraglichen s, m und n trägt, wenn nur M ein (S, R)-Bimodul und N ein R-Linksmodul ist. Diese Rechts- bzw. Linksmodulstrukturen sind im folgenden gemeint, wenn davon die Rede ist, dass $M \otimes_R N$ eine Rechts- bzw. Linksmodulstruktur trägt.

Dies bemerkt, formuliert und beweist man den folgenden Satz.

1.8. Satz. *Es seien R und S zwei Ringe mit Eins. Ferner sei M ein R-Rechtsmodul, N ein (R, S)-Bimodul und O ein S-Linksmodul. Dann ist $M \otimes_R N$ ein S-Rechtsmodul und $N \otimes O$ ein R-Linksmodul, so dass die Tensorprodukte $M \otimes_R (N \otimes_S O)$ und $(M \otimes_R N) \otimes_S O$ definiert sind. Darüber hinaus gibt es einen Isomorphismus σ von*

$$M \otimes_R (N \otimes_S O)$$

auf

$$(M \otimes_R N) \otimes_S O$$

mit

$$\sigma(m \otimes (n \otimes o)) = (m \otimes n) \otimes o$$

für alle $(m, n, o) \in M \times N \times O$.

Beweis. Es sei $m \in M$. Wir definieren die Abbildung a_m von N in $M \otimes_R N$ durch $a_m(x) := m \otimes x$ für alle $x \in N$. Dann ist a_m ein Homomorphismus des S-Rechtsmoduls N in den S-Rechtsmodul $M \otimes_R N$. Wir setzen $b_m := a_m \otimes 1_O$. Dann ist b_m ein Homomorphismus von $N \otimes_S O$ in $(M \otimes_R N) \otimes_S O$. Wir definieren nun die Abbildung f von $M \times (N \otimes_S O)$ in $(M \otimes_R N) \otimes_S O$ durch

$$f(m, z) := b_m(z)$$

für alle $m \in M$ und alle $z \in N \otimes_S O$. Die Abbildung f ist offenbar in beiden Argumenten additiv. Es gilt aber auch $f(mr, z) = f(m, rz)$ für alle in Frage kommenden m, r und z. Um dies zu beweisen, dürfen wir annehmen, dass $z = n \otimes o$ ist. Dann ist

$$\begin{aligned} f(mr, z) &= (a_{mr} \otimes 1_O)(n \otimes o) = (mr \otimes n) \otimes o = (m \otimes rn) \otimes o \\ &= (a_m \otimes 1_O)(rn \otimes o) = f(m, rn \otimes o) = f(m, rz). \end{aligned}$$

Damit ist gezeigt, dass f tensoriell ist. Es gibt also einen Homomorphismus σ von $M \otimes_R (N \otimes_S O)$ in $(M \otimes_R N) \otimes_S O$ mit $f(m, z) = \sigma(m \otimes z)$ für alle $m \in M$ und alle $z \in N \otimes_S O$. Hieraus folgt insbesondere, dass

$$\sigma(m \otimes (n \otimes o)) = (m \otimes n) \otimes o$$

für alle in Frage kommenden m, n und o gilt. Nach dem bislang Bewiesenen wird es dem Leser nicht schwer fallen zu zeigen, dass es einen Homomorphismus τ von $(M \otimes_R N) \otimes_S O$ in $M \otimes_R (N \otimes_S O)$ gibt mit

$$\tau((m \otimes n) \otimes o) = m \otimes (n \otimes o)$$

für alle m, n und o. Hieraus folgt schließlich, dass σ und τ invers zueinander sind, so dass σ in der Tat ein Isomorphismus ist.

Falls es dem Leser wider Erwarten nicht gelungen sein sollte, die Existenz von τ nachzuweisen, so findet er einen solchen Nachweis bei Bourbaki, der es allerdings dem Leser überläßt, die Existenz von σ zu beweisen.

Es sei K ein kommutativer Körper und V sei ein Rechtsvektorraum über K. Ist dann $k \in K$ und $v \in V$, so setzen wir $kv := vk$. Weil K kommutativ ist, wird V auf diese Weise zu einem K-Linksvektorraum. Es gilt sogar, dass V ein (K, K)-Bivektorraum ist. Sind nämlich $k, l \in K$ und $v \in V$, so ist

$$k(vl) = (vl)k = v(lk) = v(kl) = (vk)l = (kv)l.$$

Sprechen wir in Zukunft von einem Vektorraum V über einem kommutativen Körper K, so verstehen wir darunter immer einen (K, K)-Bivektorraum mit $kv = vk$ für alle $v \in V$ und alle $k \in K$. Mit dieser Verabredung wird dann auch das Tensorprodukt zweier Vektorräume über einem kommutativen Körper

zu einem Vektorraum über eben diesem Körper und die Verabredung, die wir über gegebene Vektorräume über kommutativen Körpern getroffen haben, dass nämlich $kv = vk$ für alle in Frage kommenden k und v gilt, gilt auch für dass Tensorprodukt der beiden Vektorräume, wie Satz 1.6 zeigt.

Macht man solche Generalvoraussetzungen, wie wir es gerade taten, so muss man natürlich vorsichtig sein, da man möglicherweise ein Objekt von der Art konstruiert, über die man die Generalvoraussetzung gemacht hat. Dann muss man zeigen, dass das Objekt auch die gewünschten Eigenschaften hat, was sicher nicht immer zutrifft. Das erinnert mich an eine Episode aus der Zeit, da meine Kinder zur Schule gingen. Meine Tochter Suzanne kam eines Tages zu mir, der ich Zeitung lesend auf dem Sofa lag, und sagte: „Papa, wir schreiben morgen eine Mathe-Arbeit. Kannst du mich abfragen?“ Ich konnte: Sie gab mir ihr Heft: Ich schaute in ihr Heft und tat das, was ich immer in zweifelhaften Situation tue, ich sagte: „Ach du meine Güte!“, und fuhr fort, „Gib mir, bitte, dein Buch.“ Im Buch stand der gleiche Unfug. Es brachte eine zweifelhafte Definition von Kardinalzahl und fuhr fort, dass jede Menge eine Kardinalzahl habe und dass die Menge der Kardinalzahlen die Menge der natürlichen Zahlen sei. Das war für mich ein gefundenes Fressen. Ich fragte sie also: „Jede Menge hat eine Kardinalzahl?“„Ja.“„Also auch die Menge der natürlichen Zahlen?“„Ja.“„Jede Kardinalzahl ist eine natürliche Zahl?“„Ja.“„Ist 10395 die Kardinalzahl der Menge der natürlichen Zahlen?“„Nein.“„Ist 23576 die Kardinalzahl der Menge der natürlichen Zahlen?“„Nein.“„Ja, was ist denn die Kardinalzahl der Menge der natürlichen Zahlen?“„Unendlich.“„Ist Unendlich eine natürliche Zahl?“„Nein.“„Was ist denn Unendlich?“„So’n Symbol.“ Ich rief also den Lehrer an und äußerte ihm meine Bedenken. Unter anderem erwähnte ich, dass es neben den natürlichen Zahlen ja auch noch andere Kardinalzahlen gäbe. Darauf der Lehrer: „Das ist natürlich richtig, aber die Mengen, die wir betrachten, sind alle endlich.“„So!“, sagte ich, „Und die Menge der natürlichen Zahlen?“„Darüber habe ich noch nicht nachgedacht.“ Die Arbeit wurde erst am übernächsten Tag geschrieben. Bei dem Buch handelte es sich um den Lambacher–Schweitzer, den Namen des Lehrers zu nennen verbietet des Sängers Höflichkeit.

Doch zurück zu unserem Thema.

1.9. Satz. *Es sei K ein kommutativer Körper und V und W seien zwei Vektorräume über K. Ist B eine Basis von V und C eine Basis von W, so ist*

$$\{b \otimes c \mid b \in B, c \in C\}$$

eine Basis von $V \otimes_K W$.

Beweis. Um diesen Satz zu beweisen, kann man sich natürlich des Satzes 1.5 bedienen. Da Wiederholung für den Lernenden aber nützlich ist, führen wir den Beweis des vorliegenden Satzes unabhängig von Satz 1.5 aus, auch wenn wir dafür einiges doppelt machen.

Es sei $v \in V$ und $w \in W$. Es gibt dann $b_1, \ldots, b_m \in B$ und $k_1, \ldots, k_m \in K$ sowie $c_1, \ldots, c_n \in C$ und $l_1, \ldots, l_n \in K$ mit $v = \sum_{i:=1}^{m} k_i b_i$ und $x = \sum_{j:=1}^{n} l_j c_j$.

Es folgt

$$v \otimes w = \sum_{i:=1}^{m} \sum_{j:=1}^{n} k_i l_j (b_i \otimes c_j).$$

Weil $V \otimes_K W$ als abelsche Gruppe von der Menge der $v \otimes w$ erzeugt wird, wird $V \otimes_K W$ auch als Vektorraum von dieser Menge erzeugt. Daher ist die Menge der $b \otimes c$ ein Erzeugendensystem des K-Vektorraumes $V \otimes_K W$.

Es sei $b \in B$ und $c \in C$. Wir definieren die linearen Abbildungen π und ρ von V bzw. W in K durch $\pi(b) := 1$ und $\pi(x) := 0$ für $x \in B - \{b\}$, bzw., $\rho(c) := 1$ und $\rho(y) := 0$ $y \in C - \{c\}$. Ferner definieren wir die Abbildung f von $V \times W$ in K durch $f(v, w) := \pi(v)\rho(w)$. Dann ist f tensoriell, so dass es eine lineare Abbildung φ von $V \otimes_K W$ in K gibt mit

$$\varphi(v \otimes w) = \pi(v)\rho(w)$$

für alle $v \in V$ und alle $w \in W$. Es folgt $\varphi(b \otimes c) = 1$ und $\varphi(x \otimes y) = 0$ für alle $(x, y) \in B \times C$ — $\{(b, c)\}$, so dass $b \otimes c$ von $B \times C$ — $\{(b, c)\}$ linear unabhängig ist. Damit ist der Satz bewiesen.

1.10. Korollar. *Es sei K ein kommutativer Körper. Sind V und W Vektorräume endlichen Ranges über K, so hat auch $V \otimes_K W$ endlichen Rang und es gilt*

$$\mathrm{Rg}_K(V \otimes_K W) = \mathrm{Rg}_K(V)\mathrm{Rg}_K(W).$$

Das Argument, welches wir zum Beweise von 1.9 verwandten, lässt sich noch einmal verwenden, was daraufhin deutet, dass eigentlich ein Satz zu formulieren sei, der dieses Argument institutionalisiert.

1.11. Satz. *Es sei K ein kommutativer Körper und V und W seien Vektorräume über K. Sind $b_1, \ldots, b_n$ linear unabhängige Vektoren aus V, sind $y_1, \ldots, y_n \in W$ und gilt*

$$\sum_{i:=1}^{n} (b_i \otimes y_i) = 0,$$

so ist $y_i = 0$ für $i := 1, \ldots, n$.

Beweis. Es sei $i \in \{1, \ldots, n\}$. Es sei $i \in \{1, \ldots, n\}$. Es gibt dann eine lineare Abbildung f von V in K mit $f(b_i) = 1$ und $f(b_j) = 0$ für alle von i verschiedenen j. Ist g irgendeine lineare Abbildung von W in K, so ist die durch $\varphi(v, w) := f(v)g(w)$ definierte Abbildung φ tensoriell. Es gibt daher eine lineare Abbildung π von $V \otimes_K W$ in K mit $\pi(v \otimes w) = f(v)g(w)$. Hieraus folgt

$$0 = \pi\left(\sum_{j:=1}^{n} b_j \otimes y_j\right) = \sum_{i:=1}^{n} f(b_j)g(y_j) = g(y_i).$$

Also ist $g(y_i) = 0$ für alle linearen Abbildungen g von W in K, so dass, wie behauptet, $y_i = 0$ ist.

2. Homomorphismen projektiver Räume

Da wir Tensorprodukte allgemeiner definiert haben, als wir sie eigentlich brauchen, werden wir von unserem Thema abweichen und zeigen, dass die allgemeinere Version des Tensorproduktes auch für die projektive Geometrie von Nutzen ist.

Ist K ein Körper und ist R ein Teilring von K mit $1 \in R$, so ist K natürlich ein (R, K)-Bimodul. Ist M ein R-Rechtsmodul, so trägt $M \otimes_R K$ nach 1.6 daher eine Struktur als K-Rechtsvektorraum, die mit der Struktur des Tensorproduktes verträglich ist. Dies machen wir uns jetzt zu Nutze.

2.1. Satz. *Es sei K ein Körper und R sei ein Teilring von K mit $1 \in R$. Ist M ein R-Rechtsmodul, so trägt $M \otimes_R K$ genau eine K-Rechtsvektorraumstruktur mit*

$$(m \otimes k)l = m \otimes (kl)$$

für alle $m \in M$ und alle $k, l \in K$. Ist M ein freier R-Modul und ist B eine R-Basis von M, so ist

$$\{b \otimes 1 \mid b \in B\}$$

eine K-Basis von $M \otimes_R K$.

Beweis. Die erste Aussage folgt, wie schon bemerkt, aus Satz 1.6.

Weil B eine Basis von M ist, ist $M = \oplus_{b \in B} bR$. Für $b \in B$ sei π_b die durch $\pi_b(b) := b$ und $\pi_b(c) := 0$ für $c \in B - \{b\}$ definierte Projektion von M auf bR. Nach 1.5 ist dann

$$M \otimes_R K = \bigoplus_{b \in B} (\pi_b \otimes 1_K)(M \otimes_R K).$$

Weil B eine Basis von M ist, wird $M \otimes_R K$ von der Menge der Elemente $c \otimes k$ mit $c \in B$ und $k \in K$ erzeugt. Daher wird

$$(\pi_b \otimes 1_K)(M \otimes_R K)$$

von den Bildern dieser Elemente unter $\pi_b \otimes 1_K$ erzeugt. Ist nun $c \in B - \{b\}$, so ist $(\pi_b \otimes 1_K)(c \otimes k) = 0$. Ferner ist

$$(\pi_b \otimes 1_K)(b \otimes k) = (b \otimes 1)k.$$

Damit ist gezeigt, dass

$$(\pi_b \otimes 1_K)(M \otimes_R K) = (b \otimes 1)K$$

ist. Um zu zeigen, dass $\{b \otimes 1 \mid b \in B\}$ eine Basis ist, ist also nur noch zu zeigen, dass die direkten Summanden allesamt von $\{0\}$ verschieden sind.

Zu diesem Zweck zitieren wir zunächst noch einmal 1.5. Nach diesem Satz ist $(\pi_b \otimes 1_K)(M \otimes_R K)$ zu $bR \otimes_R K$ isomorph. Da die durch $\beta(br, k) := rk$ definierte Abbildung β tensoriell ist, gibt es einen Homomorphismus η von $bR \otimes_R K$ in K mit $\eta(br \otimes k) = rk$ für alle $r \in R$ und alle $k \in K$. Es folgt $\eta(b \otimes 1) = 1$, so dass $(bR \otimes_R)K)$ nicht nur aus der Null besteht. Damit ist alles bewiesen.

Der Leser beachte, dass $b \otimes 1$ im letzten Absatz ein Element aus $bR \otimes_R K$ bezeichnet, während zuvor ein Element aus $M \otimes_R K$ mit diesem Ausdruck gemeint war.

2.2. Korollar. *Es sei K ein Körper und R sei ein Teilring von K mit $1 \in R$. Ist dann F ein freier Modul über R, ist $f \in F$ und gilt $f \otimes 1 = 0$, so ist $f = 0$.*

Beweis. Weil F ein freier R-Modul ist, gibt es eine Basis B von F. Es gibt dann weiter $b_1, \ldots, b_m \in B$ und $r_1, \ldots, r_m \in R$ mit $f = \sum_{i:=1}^m b_i r_i$. Es folgt

$$0 = f \otimes 1 = \sum_{i:=1}^{m} (b_i r_i \otimes 1) = \sum_{i:=1}^{m} (b_i \otimes 1) r_i,$$

so dass nach 2.1 gilt, dass $r_i = 0$ ist für alle i. Somit ist $f = 0$, wie behauptet.

2.3. Satz. *Es sei K ein Körper und R sei ein Teilring von K mit $1 \in R$. Ferner sei F ein freier Rechtsmodul über R. Ist $U \in \mathrm{L}_K(F \otimes_R K)$ und ist*

$$D := \{f \mid f \in F, f \otimes 1 \in U\},$$

so gilt: Ist $f \in F$ und $r \in R^*$ und gilt $fr \in D$, so ist $f \in D$, m.a.W., der Faktormodul F/D ist torsionsfrei.

Beweis. Wegen $fr \in D$ ist $fr \otimes 1 \in U$. Es folgt

$$f \otimes 1 = (f \otimes r) r^{-1} = (fr \otimes 1)^{-1} \in U,$$

so dass in der Tat $f \in D$ gilt.

Der Modul D kann natürlich, gemessen an U, sehr klein sein. Wir kümmern uns nun zunächst um Bedingungen, die erzwingen, dass D so groß wie möglich wird.

Die Bemerkung, dass im folgenden Satz a) eine Konsequenz von d) ist, verdanke ich Herrn U. Dempwolff. Wir benötigen des weiteren jedoch nur, dass b) aus a) folgt.

2.4. Satz. *Ist K ein Körper und ist R ein Teilring von K mit $1 \in R$, so sind die folgenden Aussagen äquivalent:*

a) *Zu jeder endlichen Teilmenge E von K gibt es ein $s \in R^*$ mit $es \in R$ für alle $e \in E$.*

b) *Ist M ein Rechtsmodul über R, sind $f_1, \ldots, f_n \in M$ und $k_1, \ldots, k_n \in K$, so gibt es $r_1, \ldots, r_n \in R$ und ein $y \in K^*$ mit*

$$\sum_{i:=1}^{n} (f_i \otimes k_i) = \left(\sum_{i:=1}^{n} f_i r_i \right) \otimes y$$

und der weiteren Eigenschaft, dass $r_i = 0$ genau dann gilt, wenn $k_i = 0$ ist.

c) *Ist M ein Rechtsmodul über R und ist $v \in M \otimes_R K$, so gibt es ein $m \in M$ und ein $k \in K^*$ mit $v = m \otimes k$.*

d) *Es gibt einen nicht endlich erzeugten freien Rechtsmodul F über R, so dass es zu jedem $v \in F \otimes_R K$ ein $f \in F$ und ein $k \in K^*$ gibt mit $v = f \otimes k$.*

Beweis. a) impliziert b): Nach Voraussetzung gibt es ein $s \in R^*$ mit $k_i s \in R$ für $i := 1, \ldots, n$. Setze $r_i := k_i s$ und $y := s^{-1}$. Dann gilt in der Tat

$$\sum_{i:=1}^{n} (f_i \otimes k_i) = \left(\sum_{i:=1}^{n} f_i r_i \right) \otimes y.$$

Wegen $r_i = k_i s$ und $s \neq 0$ gilt auch die Aussage über das Verschwinden der r_i.

Es ist trivial, dass c) eine Folge von b) und dass d) eine Folge von c) ist.

d) impliziert a): Es sei B eine Basis von F und E sei eine endliche Teilmenge von K. Wir dürfen annehmen, dass $1 \in E$ ist. Weil F nicht endlich erzeugt ist, ist B nicht endlich, so dass es eine injektive Abbildung b von E in B gibt. Setze

$$v := \sum_{e \in E} (b_e \otimes e).$$

Es gibt dann ein $f \in F$ und ein $k \in K^*$ mit $v = f \otimes k$. Es sei $f = \sum_{c \in B} c r(c)$. Dann ist

$$v = f \otimes k = \sum_{c \in B} (c \otimes 1) r(c) k.$$

Andererseits ist

$$v = \sum_{e \in E} (b_e \otimes 1) e.$$

Nach 2.1 gilt folglich $e = r(b_e)k$ für alle $e \in E$. Dann ist aber $ek^{-1} \in R$ für alle $e \in E$. Wegen $1 \in E$ folgt $k^{-1} = 1k^{-1} \in R$. Damit ist alles bewiesen.

Wir treffen des weiteren die Verabredung, mit $\Delta_R(M)$ die Menge aller Teilmoduln N des R-Rechtsmoduls M zu bezeichnen, für die M/N torsionsfrei ist. Ist Φ eine Teilmenge von $\Delta_R(M)$, so ist auch

$$\bigcap_{X \in \Phi} X \in \Delta_R(M).$$

Nach I.2.1 ist $(\Delta_R(M), \subseteq)$ also ein vollständiger Verband. Zu bemerken ist, dass die obere Grenze zweier Elemente aus $\Delta_R(M)$ auch in gut sich stellenden Fällen meist nicht die Summe dieser beiden Elemente ist. (Diese geschraubt klingende Formulierung habe ich gewählt, um darauf hinweisen zu können, dass „ill posed problems“ keine „schlecht gestellten Probleme“— so etwas gibt es nicht —, sondern „schlecht sich stellende Probleme“ sind. Wer von schlecht gestellten Problemen redet, darf sich nicht über das Deutsch unserer Studenten beklagen.)

2.5. Satz. *Es sei K ein Körper und R sei ein Teilring von K mit $1 \in R$. Ferner gebe es zu jeder endlichen Teilmenge E von K ein $r \in R^*$ mit $er \in R$ für alle $e \in E$. Schließlich sei F ein freier R-Rechtsmodul. Definiert man die Abbildung φ von $\Delta_R(F)$ in $\mathrm{L}_K(F \otimes_R K)$ durch*

$$\varphi(D) := \sum_{f \in D} (f \otimes 1)K$$

für alle $D \in \Delta_R(F)$, so ist φ ein Isomorphismus von $(\Delta_R(F), \subseteq)$ auf $(\mathrm{L}_K(F \otimes_R K), \leq)$.

Beweis. Setze $V := F \otimes_R K$. Für $U \in \mathrm{L}_K(V)$ werde $\psi(U)$ definiert durch

$$\psi(U) := \{f \mid f \in F, f \otimes 1 \in U\}.$$

Zunächst folgt

$$D \subseteq \psi\varphi(D)$$

für alle $D \in \Delta_R(F)$.

Es sei $D \in \Delta_R(F)$. Ferner sei $f \in \psi\varphi(D)$. Es gibt dann $d_1, \dots, d_n \in D$ und $k_1, \dots, k_n \in K$ mit

$$f \otimes 1 = \sum_{i:=1}^{n} (d_i \otimes k_i).$$

Nach 2.4 gibt es $r_1, \dots, r_n \in R$ und ein $y \in K^*$ mit

$$f \otimes 1 = \left(\sum_{i:=1}^{n} d_i r_i \right) \otimes y.$$

Nach Voraussetzung gibt es ein $a \in R^*$ mit $ya \in R$. Es folgt

$$fa \otimes 1 = \left(\sum_{i:=1}^{n} d_i r_i ya \right) \otimes 1.$$

Mit 2.2 erhalten wir folglich

$$fa = \sum_{i:=1}^{n} d_i r_i ya \in D.$$

Wegen $a \neq 0$ und $D \in \Delta_R(F)$ folgt daher $f \in D$. Somit ist $D = \psi\varphi(D)$.

Es sei $U \in \mathrm{L}_K(V)$. Dann ist

$$\varphi\psi(U) = \sum_{f \in F, f \otimes 1 \in U} (f \otimes 1)K.$$

Banal ist, dass $\varphi\psi(U) \leq U$ gilt. Ist andererseits $u \in U$, so folgt mit 2.4 die Existenz von $f \in F$ und $k \in K^*$ mit $u = f \otimes k$. Hieraus folgt zunächst $f \otimes 1 = uk^{-1} \in U$ und dann $u = (f \otimes 1)k \in \varphi\psi(U)$, so dass $U = \varphi\psi(U)$ ist. Damit ist gezeigt, dass φ eine Bijektion von $\Delta_R(F)$ auf $\mathrm{L}_K(V)$ ist.

Sind $D, D' \in \Delta_R(F)$ und ist $D \subseteq D'$, so ist natürlich $\varphi(D) \leq \varphi(D')$. Sind $U, U' \in \mathrm{L}_K(V)$ und ist $U \leq U'$, so folgt genauso einfach die Gültigkeit der Inklusion $\psi(U) \subseteq \psi(U')$. Damit ist der Satz bewiesen.

Dieser Satz ist bestmöglich, wie wir noch sehen werden. Andererseits kann man mehr beweisen, wenn der Rang von F endlich und R etwa ein Hauptidealbereich ist. Davon später mehr. Zunächst wollen wir nach Beispielen von Ringen suchen, die die Voraussetzungen von 2.5 erfüllen.

Ist K ein kommutativer Körper und ist R ein Teilring von K mit $1 \in R$, so erfüllt dieses Paar genau dann die Voraussetzungen von 2.5, wenn K der Quotientenkörper von R ist, so dass dieser Satz also von realen Verhältnissen handelt.

Eine weitere Situation, die im Kommutativen ein Spezialfall der gerade beschriebenen Situation ist, ist die folgende: Es sei K ein Körper und R sei ein Teilring von K mit $1 \in R$. Wir nennen R *Bewertungsring* von K, falls gilt: Ist $k \in K - R$, so ist $k^{-1} \in R$. Zeigen wir zunächst, dass für Körper mit Bewertungsringen der Satz 2.5 gilt.

2.6. Satz. *Es sei K ein Körper und R sei ein Bewertungsring von K. Ist E eine endliche Teilmenge von K, so gibt es ein $r \in R^*$ mit $er \in R$ für alle $e \in E$.*

Beweis. Ist E eine Teilmenge von R, so setzen wir $r := 1$. Wir dürfen daher annehmen, dass es ein $e \in E$ gibt, welches nicht in R liegt. Dann liegt aber $e^{-1} \in R$. Ist e das einzige Element von E, so setzen wir $r := e^{-1}$. Ist e nicht das einzige Element von E, so gibt es nach Induktionsannahme ein $s \in R^*$ mit $fe^{-1}s \in R$ für alle $f \in E - \{e\}$. Setzt man $r := e^{-1}s$, so gilt $fr \in R$ für alle $f \in E$.

Weitere Eigenschaften von Bewertungsringen sind in den nächsten beiden Sätzen notiert.

2.7. Satz. *Es sei K ein Körper und R sei ein Bewertungsring von K. Ist dann E eine endliche Teilmenge von $R^* := R - \{0\}$, so gibt es $s, t \in E$ mit $fs^{-1}, t^{-1}f \in R$ für alle $f \in E$.*

Beweis. Da $1 \in R$ gilt, ist der Satz richtig, falls E nur ein Element enthält. Es sei $|E| \geq 1$ und $e \in E$. Es gibt dann ein $\lambda \in E - \{e\}$ mit $f\lambda^{-1} \in R$ für alle $f \in E - \{e\}$. Ist $e\lambda^{-1} \in R$, so tut's $s := \lambda$. Ist $e\lambda^{-1} \notin R$, so ist $\lambda e^{-1} \in R$. In diesem Falle tut's $s := e$.

Die Existenz von t beweist sich analog.

2.8. Satz. *Es sei K ein Körper und R sei ein Bewertungsring von K. Ist dann $M := \{f \mid f \in R, f^{-1} \notin R\}$, so ist M ein zweiseitiges Ideal von R und alle von R verschiedenen Rechts- wie Linksideale sind in M enthalten.*

Beweis. M ist die Menge der Elemente von R, die keine Einheiten von R sind. Um zu zeigen, dass M ein Ideal ist, ist nur kritisch nachzuweisen, dass M additiv abgeschlossen ist. Dazu seien $a, b \in M$. Wegen Satz 2.5 dürfen wir annehmen, dass $b = ac$ ist mit $c \in R$. Dann ist aber, falls $a + b \neq 0$ ist,

$$1 = (a + b)(a + b)^{-1} = a(1 + c)(a + b)^{-1}.$$

Also ist

$$a^{-1} = (1 + c)(a + b)^{-1}.$$

Hieraus folgt $(a + b)^{-1} \notin R$, da andernfalls $a^{-1} \in R$ wäre. Also ist $a + b \in M$, was natürlich auch richtig ist, wenn $a + b = 0$ ist.

Die restlichen Aussagen folgen daraus, dass $R - M$ nur aus Einheiten von R besteht.

Für den Kenner sei hier folgendes erwähnt. Ist R ein Integritätsbereich und ist F ein freier R-Modul, so ist $\Delta_R(F)$ gerade die Menge der reinen Teilmoduln von F. Dies gesagt, ist klar, dass man im Falle von Hauptidealbereichen einige der folgenden Sätze allgemeiner formulieren kann, als wir es tun werden.

2.9. Satz. *Es sei R ein Integritätsbereich oder ein Bewertungsring. Ferner sei M ein Modul über R. Ist $T(M)$ die Menge der Torsionselemente von M, so ist M ein Teilmodul von M.*

Beweis. Für Integritätsbereiche ist die Aussage völlig banal. Es sei R also ein Bewertungsring. Ferner seien m und n Torsionselemente von M. Es gibt dann $r, s \in R^*$ mit $mr = 0 = ns$. Nach 2.7 dürfen wir annehmen, dass $s = rt$ ist mit einem $t \in R$. Es folgt

$$(m + n)s = mrt + ns = 0,$$

so dass $m + n \in T(M)$ gilt.

Es sei weiterhin $m \in T(M)$ und es sei $0 \neq s \in R$. Es gibt ein $r \in R^*$ mit $mr = 0$. Ist $r = st$ mit $t \in R$, so ist einmal $t \neq 0$ und zum anderen $(ms)t = mr = 0$, so dass $ms \in T(M)$ gilt. Ist s kein Linksteiler von r, so gibt es nach 2.7 ein $t \in R$ mit $s = rt$. In diesem Falle ist aber $ms = 0$. Damit ist alles bewiesen.

2.10. Satz. *Es sei R ein Hauptidealbereich oder ein Bewertungsring. Es sei ferner M ein torsionsfreier Rechtsmodul über R und $0 \neq m \in M$. Der Teilmodul U von M werde definiert durch $U/mR = T(M/mr)$. Ist U endlich erzeugt, so gibt es ein $u \in U$ mit $U = uR$.*

Beweis. Es sei $U = \sum_{i:=1}^n f_i R$. Es gibt dann $r_i \in R*$ und $s_i \in R$ mit $f_i r_i = m s_i$ für $i := 1, \ldots, n$. Wir dürfen natürlich annehmen, dass $f_i \neq 0$ ist. Weil M torsionsfrei ist, ist dann $f_i r_i \neq 0$ und folglich $s_i \neq 0$ für alle i.

Wir betrachten zunächst den Fall, dass R ein Hauptidealbereich ist. Dann ist R insbesondere kommutativ. Setze $a := \prod_{i:=1}^n r_i$. Ist $x \in U$, so gibt es $\lambda_i \in R$ mit $x = \sum_{i:=1}^n f_i \lambda_i$. Weil r_i auf Grund der Kommutativität von R ein Teiler von a ist, gibt es $g_i \in R$ mit $\lambda_i a = r_i g_i$. Es folgt

$$xa = \sum_{i:=1}^n f_i r_i g_i = m \sum_{i:=1}^n s_i g_i.$$

Somit ist die durch $\sigma(x) := xa$ definierte Abbildung σ zunächst eine Abbildung von U in mR. Da R kommutativ ist, ist σ sogar ein Homomorphismus von U in mR. Weil a nicht Null und M torsionsfrei ist, ist σ sogar ein Monomorphismus. Nun ist mR aber ein epimorphes Bild von R. Weil R ein Hauptidealbereich ist, wird folglich jeder Teilmodul von mR von einem Element erzeugt. Daher wird $\sigma(U)$ und damit U von einem Element erzeugt.

Es sei nun R ein Bewertungsring. Ist $n = 1$, so ist nichts zu beweisen. Es sei also $n > 1$. Auf Grund von 2.7 dürfen wir annehmen, dass $s_{n-1} = s_n t$ mit $t \in R$ ist. Dann ist aber

$$f_{n-1} r_{n-1} = m s_n t = f_n r_n t.$$

nach 2.7 ist r_{n-1} ein Rechtsteiler von $r_n t$ oder $r_n t$ ein Rechtsteiler von r_{n-1}. Wegen der Torsionsfreiheit von M gilt im ersten Falle $f_{n-1} \in f_n R$ und im zweiten Falle $f_n \in f_{n-1} R$. Induktion führt nun zum Ziele.

Der Leser, der mit den Feinheiten von ggT-Bereichen vertraut ist, wird sehen, dass man bei der folgenden Definition und einigen der weiteren Sätze statt Hauptidealbereich auch ggT-Bereich sagen könnte. Da die wesentlichen Sätze für ggT-Bereiche jedoch ihre Gültigkeit verlieren, verzichten wir bei den fraglichen Sätzen auf die größere Allgemeinheit.

Es sei R ein Hauptidealbereich oder ein Bewertungsring. Ferner sei F ein freier R-Rechtsmodul und B sei eine Basis von F. Ist $f \in F$, so gibt es eine Abbildung r von B in R mit endlichem Träger, so dass $f = \sum_{b \in B} b r_b$ gilt. Ist R ein Hauptidealbereich, so setzen wir

$$\mathrm{cont}(f) := \mathrm{ggT}(r_b \mid b \in B).$$

Ist R ein Bewertungsring, so gibt es nach 2.7 ein $b \in B$ mit $r r_b^{-1} \in R$ für alle $c \in B$, da der Träger von r ja endlich ist. In diesem Falle setzen wir

$$\mathrm{cont}(f) := r_b.$$

Wir nennen $\mathrm{cont}(f)$ den *Inhalt* von f. Der Inhalt $\mathrm{cont}(f)$ von f ist bis auf Einheiten eindeutig bestimmt. Ist $\mathrm{cont}(f) = 1$, so nennen wir f *primitiv*.

Es sei C eine weitere Basis von F. Ist $c = \sum_{b \in B} b A_{bc}$, und $f = \sum_{c \in C} c\lambda_c$, so ist

$$f = \sum_{b \in B} b \sum_{c \in C} A_{bc}\lambda_c.$$

Hieraus folgt, dass der mit Hilfe von C definierte Inhalt von f ein Teiler des mit Hilfe von B definierten Inhalts von f ist. Vertauscht man in diesem Argument die Rollen von B und C, so sieht man, dass auch der mittels B definierte Inhalt ein Teiler des mittels C definierten Inhalts ist. Somit hängt die Funktion cont nicht von der Wahl der Basis ab.

2.11. Satz. *Es sei R ein Hauptidealbereich oder ein Bewertungsring. Ist F ein freier Rechtsmodul über R und ist $f \in F$ primitiv, so ist $fR \in \Delta_R(F)$. Ist $0 \neq g \in F$, so gibt es ein primitives $f \in F$ mit $g = f\mathrm{cont}(g)$.*

Beweis. Es sei B eine Basis von F. Dann ist $f = \sum_{b \in B} b\alpha_b$, wobei α eine Abbildung von B in R ist, deren Träger endlich ist. Es sei $0 \neq h \in F$ und $s \in R^*$ und es gelte $hs \in fR$. Es gibt dann wegen der Torsionsfreiheit von F (Satz 2.2) ein $t \in R^*$ mit $hs = ft$. Ferner ist $h = \sum_{b \in B} b\beta_b$ und es folgt

$$\sum_{b \in B} b\beta_b s = hs = ft = \sum_{b \in B} b\alpha_b t$$

und damit $\beta_b s = \alpha_b t$ für alle $b \in B$.

Ist R ein Hauptidealbereich, so ist

$$\mathrm{cont}(h)s = \mathrm{ggT}(\beta_b s \mid b \in B) = \mathrm{ggT}(\alpha_b t \mid b \in B) = \mathrm{cont}(f)t = t.$$

Ist R ein Bewertungsring, so gibt es ein b, so dass α_b eine Einheit ist, da f ja primitiv ist. Es folgt $t = \alpha_b^{-1}\beta_b s$ und weiter $h = f\alpha_b^{-1}\beta_b \in fR$. Damit ist gezeigt, dass $fR \in \Delta_R(F)$ gilt.

Es sei $g = \sum_{b\in B} br_b$. Setze $f := \sum_{b\in B} br_b \mathrm{cont}(g)^{-1}$. Dann ist f primitiv und $g = f\mathrm{cont}(g)$.

2.12. Satz. *Es sei R ein Ring. Ferner sei M ein Rechtsmodul über R und U sei ein Teilmodul von M. Ist M/U ein freier R-Modul, so ist U ein direkter Summand von M.*

Beweis. Mit Hilfe des Auswahlaxioms erhalten wir eine Familie B von Elementen von M, so dass $\{b + U \mid b \in B\}$ eine Basis von M/U ist. Wir setzen

$$V := \sum_{b\in B} bR.$$

Natürlich gilt $M = U + V$. Es sei $u \in U \cap V$. Es gibt dann $b_1, \ldots, b_n \in B$ und $r_1, \ldots, r_n \in R$ mit $u = \sum_{i:=1}^n b_i r_i$. Es folgt

$$U = u + U = \sum_{i:=1}^{n} (b_i + u) r_i.$$

Also ist $r_i = 0$ für alle i, so dass $u = 0$ und folglich $M = U \oplus V$ gilt.

2.13. Satz. *Es sei R ein Hauptidealbereich oder ein Bewertungsring. Ist M ein endlich erzeugter, torsionsfreier Rechtsmodul über R, so ist M frei in endlich vielen Erzeugenden.*

Beweis. Es sei $M = \sum_{i:=1}^n f_i R$. Ist $n = 1$, so ist M frei in einer Erzeugenden. Es sei also $n > 1$. Der Teilmodul U von M werde definiert durch $U/f_nR = T(M/f_nR)$. Dann ist M/U ein torsionsfreier R-Rechtsmodul, der von $f_1 + U, \ldots, f_{n-1} + U$ erzeugt wird. Nach Induktionsannahme ist M/U frei in höchstens $n-1$ Erzeugenden. Weil M/U frei ist, ist U nach 2.12 ein direkter Summand von M. Es sei C ein Komplement von U. Dann ist also $M = U \oplus C$ und somit $M/C \cong U$. Dies besagt, dass U endlich erzeugt ist. Mit 2.10 folgt, dass es ein $u \in U$ gibt mit $U = uR$. Da C wegen $C \cong M/U$ frei ist, ist auch M frei und zwar in höchstens n Erzeugenden.

2.14. Satz. *Es sei R ein Hauptidealbereich oder ein Bewertungsring. Ferner sei F ein freier Rechtsmodul über R. Ist D ein direkter Summand von F, so ist $D \in \Delta_R(F)$.*

Genau dann besteht $\Delta_R(F)$ genau aus den direkten Summanden von F, wenn F endlich erzeugt ist.

Beweis. Es sei D ein direkter Summand von F. Weil F frei und somit torsionsfrei ist, ist jedes Komplement von D torsionsfrei. Dies impliziert, dass auch F/D torsionsfrei ist. Folglich gilt $D \in \Delta_R(F)$.

Der Modul F sei endlich erzeugt. Ferner sei $D \in \Delta_R(F)$. Dann ist F/D endlich erzeugt, da F es ist, und nach Definition von $\Delta_R(F)$ ist F/D torsionsfrei. Nach 2.13 ist F/D daher frei, was nach 2.12 impliziert, dass D ein direkter

Summand von F ist. Ist F endlich erzeugt, so besteht $\Delta_R(F)$ also genau aus den direkten Summanden von F.

Ist R Bewertungsring, so sei R Bewertungsring des Körpers K. Ist R Hauptidealbereich, so sei K der Quotientenkörper von R. In beiden Fällen sei p ein Element von R, welches keine Einheit sei. Wir setzen

$$M := \sum_{i:=0}^{\infty} p^{-i} R.$$

Der Modul F sei nicht endlich erzeugt. Ist B eine Basis von F, so ist B nicht endlich, enthält also eine abzählbare Teilmenge C. Es sei a eine mit 0 beginnende Abzählung von C. Es gibt dann einen Epimorphismus ϵ von F auf M mit $\epsilon(a_i) := p^{-i}$ für alle nicht negativen ganzen Zahlen i und $\epsilon(b) = 0$ für alle $b \in B - C$. Es sei D der Kern von ϵ. Dann ist F/D zu M isomorph, also nicht torsionsfrei. Daher ist $D \in \Delta_R(F)$.

Wir nehmen nun an, D hätte ein Komplement G, und fahren im Indikativ fort. Dann ist G zu M isomorph. Es gibt daher eine Folge z auf G mit $G = \sum_{i:=0}^{\infty} z_i R$ und $z_{i+1} p = z_i$ für alle i. Nach 2.11 gibt es ein primitives $f \in F$ mit $z_0 = f$ cont (z_0). Weil G ein direkter Summand ist, ist $G \in \Delta_R(F)$, so dass $f \in G$ ist. Weil f primitiv ist, ist fR nach 2.11 ein Element von $\Delta_R(F)$. Nun ist $z_i p^i = z_0 \in fR$ und folglich $z_i \in fR$ für alle i. Also ist $G = fR$. Weil G und M isomorph sind, gibt es ein $v \in M$ mit $M = vR$. Es gibt weiter $r_0, \ldots, r_n \in R$ mit

$$v = \sum_{i:=0}^{n} p^{-i} r_i.$$

Es gibt außerdem ein $s \in R$ mit

$$p^{-n-1} = vs.$$

Hieraus folgt

$$1 = p^{n+1} p^{-n-1} = p \sum_{i:=0}^{n} p^{n-i} r_i s,$$

so dass p eine Einheit ist. Dies widerspricht aber der Wahl von p, so dass D doch kein direkter Summand von F ist. Damit ist alles bewiesen.

Der Leser hat hoffentlich bemerkt, dass der Satz falsch ist. Unterräume von Vektorräumen sind stets direkte Summanden, so dass man also noch voraussetzen muss, dass R kein Körper ist. Beim Beweis des Satzes haben wir ja ein von Null verschiedenes Element von R benötigt, welches in R keine Einheit ist.

Der Kern D von ϵ ist eine Hyperebene von $\Delta_R(F)$. Um dies zu beweisen, überlege sich der Leser, dass je zwei Elemente des Moduls M und damit je zwei Elemente des Moduls R/D über R linear abhängig sind. Hieraus folgt, dass D unter der in 2.5 definierten Abbildung φ auf eine Hyperebene von $F \otimes_R K$ abgebildet wird, wobei K der Quotientenkörper von R ist, falls R ein Hauptidealbereich ist, bzw. ein Körper, von dem R ein Bewertungsring ist. Es gibt

also Hyperebenen und damit Unterräume endlichen Ko-Ranges in $\Delta_R(F)$, die keine direkten Summanden sind, falls F nicht endlich erzeugt ist. Am unteren Ende des Verbandes $\Delta_R(F)$ herrschen andere Verhältnisse, wie der nächste Satz lehrt.

2.15. Korollar. *Es sei R ein Hauptidealbereich oder ein Bewertungsring. Ferner sei F ein freier Rechtsmodul über R. Ist $D \in \Delta_R(F)$ endlich erzeugt, so ist D ein direkter Summand von F.*

Beweis. Es sei B eine Basis von F. Weil D endlich erzeugt ist, gibt es eine endliche Teilmenge E von B mit

$$D \subseteq \sum_{b \in E} bR.$$

Setzt man die Summe rechter Hand gleich U, so ist U ein direkter Summand von F, da das Komplement von E in B ein Komplement von U in F erzeugt. Ferner ist $D \in \Delta_R(U)$, so dass D nach 2.14 ein direkter Summand von U ist. Dann ist aber auch ein direkter Summand von F.

2.16. Korollar. *Es sei R ein Hauptidealbereich oder ein Bewertungsring. Ferner sei F ein freier Rechtsmodul über R. Ist D ein endlich erzeugter direkter Summand von F, so ist auch jedes Komplement von D in F frei.*

Beweis. Wie beim Beweise von 2.15 sehen wir, dass D in einem endlich erzeugten direkten Summanden U von F liegt, der ein Komplement besitzt, welches frei ist. Wegen $D \in \Delta_R(F)$ folgt mit 2.14, dass D auch ein direkter Summand von U ist. Nach 2.13 ist jedes Komplement von D in U frei. Stückelt man ein solches mit dem freien Komplement von U zusammen, so erhält man ein Komplement von D, welches ein freier Modul ist. Dann ist aber auch M/D frei und folglich jedes Komplement von D.

2.17. Satz. *Es sei R ein Ring mit Eins und M sei ein zweiseitiges Ideal von R und R/M sei ein Körper. Ist F ein Rechtsmodul über R, so bezeichnen wir mit FM den von allen fm mit $f \in F$ und $m \in M$ erzeugten Teilmodul von F. Dann ist F/FM ein Rechtsvektorraum über R/M. Ist F frei und ist B eine Basis von F, so ist*

$$\{b + FM \mid b \in B\}$$

eine Basis von F/FM.

Beweis. Es ist natürlich klar, dass $\{b+FM \mid b \in B\}$ ein Erzeugendensystem von F/FM ist. Es ist also nur zu zeigen, dass dieses Erzeugendensystem auch linear unabhängig ist. Dazu sei C eine endliche Teilmenge von B und es gelte

$$\sum_{c \in C} (c + FM)(r_c + M) = 0,$$

wobei die r_c Elemente von R sind. Dann ist

$$\sum_{c \in C} cr_c \in FM.$$

Es gibt also $f_1, \ldots, f_n \in F$ und $m_1, \ldots, m_n \in M$ mit

$$\sum_{c \in C} c r_c = \sum_{i:=1}^{n} f_i m_i.$$

Stellt man nun die f_i mittels der Basis B dar, so erhält man

$$f_i = \sum_{b \in B} b \lambda_{ib}$$

mit $\lambda_{ib} \in R$ für alle i und alle b. Es folgt

$$\sum_{c \in C} c r_c = \sum_{i:=1}^{n} \sum_{b \in B} b \lambda_{ib} m_i = \sum_{b \in B} b \sum_{i:=1}^{n} \lambda_i b m_i.$$

Koeffizientenvergleich — hier benutzen wir, dass B eine Basis ist — liefert $r_c \in M$ für alle $c \in C$. Damit ist alles bewiesen.

Hat ein Ring R ein zweiseitiges Ideal M, so dass R/M ein Körper ist, so ist der Rang eines freien Moduls über R eine Invariante, wie der gerade bewiesene Satz zeigt.

Bei einem Vektorraum ist der geometrische Rang eines Unterraumes gleich seinem Rang als Vektorraum. Bei freien Moduln über Ringen, wie wir sie betrachten, ist der entsprechende Sachverhalt ganz und gar nicht evident. Daher liest sich der nächste Satz etwas umständlich.

2.18. Satz. *Es sei R ein Hauptidealbereich oder ein Bewertungsring und M sei ein maximales Ideal von R. Dann ist R/M ein Körper. Es sei weiterhin F ein freier Rechtsmodul über R und FM bezeichne wieder den von allen fm mit $f \in F$ und $m \in M$ erzeugten Teilmodul von F. Für $D \in \Delta_R(F)$ setzen wir*

$$\epsilon(D) := (D + FM)/FM.$$

Dann ist ϵ ein Epimorphismus des projektiven Verbandes

$$(\Delta_R(F), \subseteq)$$

auf den projektiven Verband

$$(\mathrm{L}_{R/M}(F/FM), \leq)$$

mit den folgenden Eigenschaften:

a) *Ist k eine natürliche Zahl, ist $D \in \Delta_R(F)$ als Modul endlich erzeugt und hat D als Modul den Rang k, so hat auch $\epsilon(D)$ den Rang k.*

b) *Ist k eine natürliche Zahl und hat $U \in \mathrm{L}_{R/M}(F/FM)$ den Rang k, so gibt es ein $D \in \Delta_R(F)$ mit $\epsilon(D) = U$. Ist $D \in \Delta_R(F)$ und gilt $\epsilon(D) = U$, so ist D als Modul endlich erzeugt und k ist auch der Rang von D.*

c) *Ist G eine Gerade von $\Delta_R(F)$, so gibt es drei Punkte auf G, deren Bilder unter ϵ paarweise verschieden sind.*

Beweis. Natürlich ist ϵ ein Homomorphismus. Dass ϵ surjektiv ist, beweisen wir erst zum Schluß.

a) Da D erzeugt ist, ist D frei, so dass klar ist, was es bedeutet, dass der Rang von D gleich k ist, nämlich, dass D eine Basis C der Kardinalität k hat. (Man kann Rang auch für torsionsfreie Moduln ohne Mühe definieren, was wir hier jedoch nicht tun.)

Nach 2.15 ist D ein direkter Summand und nach 2.16 ist jedes Komplement von D frei. Es gibt daher eine Basis B von F mit $C \subseteq B$. Nach 2.17 ist $\{b + FM \mid b \in B\}$ eine Basis von F/FM, so dass $\{\gamma + FM \mid \gamma \in C\}$ linear unabhängig ist. Da $\epsilon(D)$ von dieser Menge erzeugt wird, gilt die Behauptung a).

b) Es sei zunächst $k = 1$. Dann gibt es ein $p \in F$, so dass U von $p + FM$ erzeugt wird. Nach 2.11 gibt es ein primitives f mit $p = f\mathrm{cont}(p)$. Es folgt $\mathrm{cont}(p) \notin M$, so dass U auch von $f + FM$ erzeugt wird. Nach 2.11 ist $fR \in \Delta_R(F)$. Also ist ϵ auf fR anwendbar und wir erhalten $\epsilon(fR) = U$.

Nun sei k beliebig. Es gibt dann primitive $f_1, \ldots, f_k \in F$, so dass $\epsilon(f_1R), \ldots, \epsilon(f_kR)$ eine Basis von U ist. (Projektive Interpretation!) Es sei W das Supremum der $f_1R_1, \ldots, f_kR$ in $\Delta_R(F)$. Weil W von k Punkten erzeugt wird, ist der Rang von W als projektiver Raum höchstens gleich k. Dann ist aber auch der Rang von $\epsilon(W)$ höchstens gleich k. Nun ist $U \leq \epsilon(W)$, da ja $\epsilon(f_iR) \leq \epsilon(W)$ für alle i gilt. Daher ist $U = \epsilon(W)$ und der Rang von W als projektiver Raum ist gleich k.

Es sei B eine Basis von F. Dann hängt die Menge der f_i von einer endlichen Teilmenge von B ab. Daher liegen die f_iR in einem endlich erzeugten direkten Summanden von F. Weil W das Supremum der f_iR ist, liegt auch W in diesem direkten Summanden. Dann ist aber W auch als Modul endlich erzeugt und k ist der Rang von W als Modul.

c) Es sei G eine Gerade von $\Delta_R(F)$. Wie der Beweis von b) zeigt, ist G ein freier Modul des Ranges 2. Es gibt also eine Basis b_1, b_2 von G. Dann sind aber auch $b_1 + b_2, b_1$ und $b_1 + b_2, b_2$ Basen von G. Weil G ein direkter Summand ist, gibt es Basen B_0, B_1 und B_2 von F, die der Reihe nach die drei zuvor genannten Basen von G enthalten. Hieraus folgt dann mit 2.17, dass $\epsilon(b_1R), \epsilon((b_1 + b_2)R)$ und $\epsilon(b_2R)$ drei verschiedene Punkte sind, deren Urbilder auf G liegen.

Es bleibt die Surjektivität von ϵ nachzuweisen. Dazu sei U ein Teilraum von F/FM. Ferner sei B eine Basis des projektiven Raumes $\mathrm{L}_{R/M}(U)$. Es gibt dann eine Punktmenge C von $\Delta_R(F)$, so dass die Einschränkung von ϵ auf C eine Bijektion von C auf B ist. Es sei D das Erzeugnis von C in $\Delta_R(F)$. Ist P ein Punkt auf D, so gibt es eine endliche Teilmenge E von C, so dass P von E abhängt. Ist X der von E aufgespannte Teilraum von $\Delta_R(F)$, so hat X höchstens den Rang $|E|$. Andererseits hat $Y := \sum_{e \in E} \epsilon(eR)$ genau den Rang $|E|$. Wegen $Y \subseteq \epsilon(X)$ hat X daher ebenfalls den Rang $|E|$ und es gilt $Y = \epsilon(X)$. Hieraus folgt

$$\epsilon(P) \subseteq Y \subseteq U.$$

Weil $\epsilon(D)$ von seinen Punkten erzeugt wird, folgt mit a) und b), dass $\epsilon(D) \subseteq U$ gilt. Andererseits ist banalerweise $U \subseteq \epsilon(D)$, so dass in der Tat $U = \epsilon(D)$ ist. Damit ist ϵ auch als surjektiv erkannt.

Es gilt auch die Umkehrung dieses Satzes: Ist V ein Vektorraum über dem Körper K und ist der Rang von V mindestens 3, so lässt sich jeder Epimorphismus von $\mathrm{L}_K(V)$ auf einen projektiven Verband L, der die Menge der Punkte von $\mathrm{L}_K(V)$ auf die Menge der Punkte von $\mathrm{L}_K(V)$ auf die Menge der Punkte von L und die Menge der Geraden von $\mathrm{L}_K(V)$ auf die Menge der Geraden von L abbildet, mittels eines Bewertungsringes von K auf die obige Weise beschreiben. Einen Beweis für diesen Sachverhalt findet der Leser in Machala (1975). Machalas Beweis ist mehrere Seiten lang. Ich kann ihn zwar nachvollziehen, da er mir sein Geheimnis, weshalb er korrekt ist, aber nicht preisgibt, ist er hier nicht abgedruckt.

3. Segresche Mannigfaltigkeiten

Nach diesem Intermezzo über Epimorphismen von projektiven Verbänden wenden wir uns wieder unserem eigentlichen Thema zu.

Ist R ein kommutativer Ring mit Eins und ist M ein R-Modul, so dürfen und werden wir annehmen, dass M sowohl ein Rechts- als auch ein Linksmodul über R ist und dass darüber hinaus $rm = mr$ für alle $r \in R$ und alle $m \in M$ gilt. Dann ist M sogar ein R-Bimodul.

Es sei R ein kommutativer Ring mit Eins und $M_1, \ldots, M_t$ seien R-Moduln. Eine Abbildung f von $M_1 \times \cdots \times M_t$ in den R-Modul N heißt *t-fach linear* oder kurz *multilinear*, falls f in jedem Argument linear ist.

War das Tensorprodukt bislang eine binäre Operation, so führen wir nun das Tensorprodukt als t-äre Operation ein, um dann zu sehen, dass sich die neue Operation auf die alte zurückführen lässt. Dazu sei R ein kommutativer Ring mit Eins und $M_1, \ldots, M_t$ und T seien Moduln über R. Es sei ferner τ t-fach lineare Abbildung von $M_1 \times \cdots M_t$ in T. Wir nennen (T, τ) ein *Tensorprodukt* von $M_1, \ldots, M_t$, falls gilt:

1) Der Modul T wird von der Menge der $\tau(m_1, \ldots, m_t)$ mit $m_i \in M_i$ für $i := 1, \ldots, t$ erzeugt.
2) Ist N ein R-Modul und ist f eine multilineare Abbildung von $M_1 \times \cdots M_t$ in N, so gibt es eine lineare Abbildung g von T in N mit $f = g\tau$.

Die Frage nach Existenz und Eindeutigkeit von Tensorprodukten beantwortet der folgende Satz.

3.1. Satz. *Es sei R ein kommutativer Ring mit Eins. Sind $M_1, \ldots, M_t$ Moduln über R, so gibt es bis auf Isomorphie genau ein Tensorprodukt (T, τ) von $M_1, \ldots, M_t$.*

Beweis. Dass es bis auf Isomorphie höchstens ein Tensorprodukt gibt, beweist man wie bei solch universellen Objekten üblich.

Natürlich ist (M_1, id) ein Tensorprodukt von M_1, so dass der Satz für $t = 1$ richtig ist. Es sei $t > 1$ und $1 \leq i < t$. Nach Induktionsannahme gibt es ein Tensorprodukt (A, α) von $M_1, \ldots, M_i$ und ein Tensorprodukt (B, β) von $M_{i+1}, \ldots, M_t$. Wir zeigen, dass $(A \otimes_R B, \tau)$, wobei τ die durch

$$\tau(x_1, \ldots, x_t) := \alpha(x_1, \ldots, x_i) \otimes \beta(x_{i+1}, \ldots, x_t)$$

definierte Abbildung ist, ein Tensorprodukt von $M_1, \ldots, M_t$ ist.

Um dies zu zeigen, sei f eine multilineare Abbildung von $M_1 \times \cdots \times M_t$ in W. Ferner sei $x \in M_1 \times \cdots \times M_i$ und $y \in M_{i+1} \times \cdots \times M_t$. Wir definieren g_x durch

$$g_x(y) := f(x, y).$$

Dann ist g_x multilinear, so dass es eine lineare Abbildung ψ_x von B in W gibt mit $g_x = \psi_x \beta$.

Es sei $b \in B$. Wir definieren h_b durch

$$h_b(x) := \psi_x(b)$$

für alle $x \in M_1 \times \cdots \times M_i$. Weil ψ_x ein Homomorphismus ist und weil B von der Menge der $\beta(y)$ erzeugt wird, folgt, dass auch h_b multilinear ist. Es gibt daher einen Homomorphismus φ_b von A in W mit $h_b = \varphi_b \alpha$. Wir definieren nun die Abbildung F von $A \times B$ in W durch

$$F(a, b) := \varphi_b(a).$$

Dann ist F gewiss linear in a. Ist $x \in M_1 \times \cdots \times M_i$, so folgt

$$F(\alpha(x), b) = \varphi_b \alpha(x) = h_b(x) = \psi_x(b),$$

so dass F auch in b linear ist, da F in a linear ist und die $\alpha(x)$ den Modul A erzeugen. Schließlich ist

$$F(a, rb) = F(a, br) = F(a, b)r = F(ar, b),$$

so dass F tensoriell ist. Es gibt daher eine lineare Abbildung G von $A \otimes_R B$ in W mit $F(a, b) = G(a \otimes b)$ für alle $a \in A$ und alle $b \in B$. Mit diesem G folgt schließlich

$$\begin{aligned}(G\tau)(x, y) &= G(\alpha(x) \otimes \beta(y)) = F(\alpha(x), \beta(y)) \\ &= \psi_x(\beta(y)) = g_x(y) = f(x, y).\end{aligned}$$

Um zu erkennen, dass $(A \otimes_R B, \tau)$ ein Tensorprodukt von $M_1, \ldots, M_t$ ist, ist nur noch zu bemerken, dass die Menge der $\tau(x)$ mit $x \in M_1 \times \cdots \times M_t$ ein Erzeugendensystem von $A \bigotimes_R B$ ist. Damit ist Satz 3.1 bewiesen.

Wir haben viel mehr bewiesen als im Satz formuliert. Um dies deutlich zu machen, vereinbaren wir zunächst, statt $\tau(x_1, \ldots, x_t)$ wie üblich $x_1 \otimes \cdots \otimes x_t$ zu schreiben und das Tensorprodukt selbst mit $\bigotimes_{i:=1}^t M_i$ zu bezeichnen.

3.2. Korollar. *Es sei R ein kommutativer Ring mit Eins und $M_1, \ldots, M_t$ seien Moduln über R. Ferner sei $1 \leq i \leq t$. Es gibt dann genau einen Isomorphismus σ des Tensorproduktes $\bigotimes_{k:=1}^t M_k$ auf das Tensorprodukt $(\bigotimes_{k:=1}^i M_k) \otimes (\bigotimes_{k:=i+1}^t M_k)$ mit*

$$\sigma(x_1 \otimes \cdots \otimes x_t) = (x_1 \otimes \cdots \otimes x_i) \otimes (x_{i+1} \otimes \cdots \otimes x_t).$$

Dabei ist das Tensorprodukt über eine leere Indexmenge (hier der Fall $i = t$) als der Ring R zu interpretieren.

Beweis. Nur der Fall $i = t$ bedarf eines Hinweises. In diesem Falle wende man Satz 1.7 an.

Dieses Korollar macht explizit, dass sich das Tensorprodukt von mehreren Moduln über einem kommutativen Ring mit Hilfe des Tensorproduktes von zwei Moduln ausdrücken lässt.

Wir betrachten nun Vektorräume $V_1, \ldots, V_t$ über einem kommutativen Körper K. Die Vektoren der Form $v_1 \otimes \cdots \otimes v_t$ des Tensorproduktes $\bigotimes_{i:=1}^t V_i$ nennen wir *reine* oder auch *zerlegbare Tensoren*. Die Menge der von reinen Tensoren aufgespannten Punkte von $\mathrm{L}_K(\bigotimes_{i:=1}^t V_i)$ bezeichnen wir mit $S(V_1, \ldots, V_t)$. Wir nennen diese Menge *Segresche Mannigfaltigkeit mit den Parameterräumen* $V_1, \ldots, V_t$. Es gilt nun

3.3. Satz. *Es sei K ein kommutativer Körper und $V_1, \ldots, V_t$ seien Vektorräume über K. Ist $\pi \in S_t$, so gibt es eine projektive Kollineation κ von $\mathrm{L}_K(\bigotimes_{i:=1}^t V_i)$ auf $\mathrm{L}_K(\bigotimes_{i:=1}^t V_{\pi(i)})$ mit $S(V_1, \ldots, V_t)^\kappa = S(V_{\pi(1)}, \ldots, V_{\pi(t)})$.*

Beweis. Die Abbildung, die dem Element $(v_1, \ldots, v_t)$ das Element $v_{\pi(1)} \otimes \cdots \otimes v_{\pi(t)}$ zuordnet, ist multilinear. Es gibt daher eine lineare Abbildung λ von $\bigotimes_{i:=1}^t V_i$ auf $\bigotimes_{i:=1}^t V_{\pi(i)}$ mit

$$(v_1 \otimes \cdots \otimes v_t)^\lambda = v_{\pi(1)} \otimes \cdots \otimes v_{\pi(t)}.$$

Vertauschen der Rollen der beiden Tensorprodukte liefert die Existenz der zu λ inversen Abbildung. Folglich ist λ ein Isomorphismus und der von λ induzierte Isomorphismus κ von $\mathrm{L}_k(\bigotimes_{i:=1}^t V_i)$ auf $\mathrm{L}_K(\bigotimes_{i:=1}^t V_{\pi(i)})$ bildet $S(V_1, \ldots, V_t)$ auf $S(V_{\pi(1)}, \ldots, V_{\pi(t)})$ ab.

Es sei P ein Punkt der Segremannigfaltigkeit $S(V_1, \ldots, V_t)$ mit den Parameterräumen $V_1, \ldots, V_t$. Es gibt dann Vektoren $p_i \in V_i$ mit $P = (p_1 \otimes \cdots \otimes p_t)K$. Für $i := 1, \ldots, t$ setzen wir

$$U_i(P) := \{p_1 \otimes \cdots \otimes p_{i-1} \otimes x \otimes p_{i+1} \otimes \cdots \otimes p_t \mid x \in V_i\}.$$

Dann ist $U_i(P)$ ein zu V_i isomorpher Unterraum von $\mathrm{L}_K(\bigotimes_{i:=1}^t V_i)$, der P enthält und dessen Punkte alle zu $S(V_1, \ldots, V_t)$ gehören. Um dies anzudeuten, schreiben wir auch $U_i(P) \leq S(V_1, \ldots, V_t)$, obgleich das formal nicht korrekt ist. Wir setzen ferner

$$T(P) := \sum_{i:=1}^t U_i(P)$$

und nennen $T(P)$ den *Tangentialraum* von $S(V_1, \ldots, V_t)$ in P.

3.4. Satz. *Es sei K ein kommutativer Körper und $V_1, \ldots, V_t$ seien Vektorräume über K. Ist X eine nicht leere Teilmenge von $\{1, \ldots, t\}$ und ist $j \in \{1, \ldots, t\} - X$, so ist*

$$U_j(P) \cap \sum_{i \in X} U_i(P) = P.$$

Beweis. Auf Grund von 3.3 dürfen wir annehmen, dass $j = 1$ und $X = \{2, \ldots, s\}$ ist. Es sei $P = (p_1 \otimes \cdots \otimes p_t)K$. Ferner sei $u \in U_1(P) \cap \sum_{i:=2}^{s} U_i(P)$. Es gibt dann $x_i \in V_i$ mit

$$u = -x_1 \otimes p_2 \otimes \cdots \otimes p_t$$

einerseits und

$$u = p_1 \otimes x_2 \otimes \cdots \otimes p_t + \cdots + p_1 \otimes \cdots \otimes x_s \otimes \cdots \otimes p_t$$

andererseits. Hieraus folgt weiter unter Zuhilfenahme von 3.2, dass

$$0 = x_1 \otimes (p_2 \otimes \cdots \otimes p_t) + p_1 \otimes y$$

ist, wobei y eine naheliegende Abkürzung ist. Weil $p_2 \otimes \cdots \otimes p_t$ nicht Null ist, sind x_1 und p_1 nach 1.11 linear abhängig. Daher ist $x_1 \in p_1K$, so dass der Satz bewiesen ist.

3.5. Korollar. *Die Voraussetzungen seien die gleichen wie in Satz 3.4. Sind überdies die Ränge der V_i endlich und setzt man $r_i := \mathrm{Rg}_K(V_i)$, so ist*

$$\mathrm{Rg}_K(T(P)) = 1 - t + \sum_{i:=1}^{t} r_i.$$

Dies folgt unter Benutzung der Rangformel mittels Induktion aus 3.4.

Der nächste Satz wird seine Bedeutung verlieren, sobald Satz 3.9 bewiesen ist. Für den Beweis dieses Satzes wird er jedoch benötigt.

3.6. Satz. *Es sei K ein kommutativer Körper, $V_1, \ldots, V_t$ seien Vektorräume über K, und P sei ein Punkt von $S(V_1, \ldots, V_t)$. Ist $U \in \mathrm{L}_K(\otimes_{i:=1}^{t} V_i)$, ist $U \leq T(P)$ und liegt jeder Punkt von U auf $S(V_1, \ldots, V_t)$, so gibt es ein i mit $U \leq U_i(P)$.*

Beweis. Es sei $P = (p_1 \otimes \cdots \otimes p_t)K$ und $Q = (q_1 \otimes \cdots \otimes q_t)K$ sei ein Punkt von U. Es gibt dann $u_i \in V_i$ mit

$$-q_1 \otimes \cdots \otimes q_t = \sum_{i:=1}^{t} p_1 \otimes \cdots \otimes u_i \otimes \cdots \otimes p_t.$$

Wir dürfen $P \neq Q$ annehmen. Es gibt dann ein i mit $q_i \notin p_iK$. Wegen 3.3 dürfen wir annehmen, dass $i = 1$ ist. Dann folgt

$$0 = q_1 \otimes (q_2 \otimes \cdots \otimes q_t) + u_1 \otimes (p_2 \otimes \cdots \otimes p_t) + p_1 \otimes y,$$

wobei y wieder für einen längeren Ausdruck steht, dessen Einzelheiten uns nicht interessieren. Weil $q_2 \otimes \cdots \otimes q_t$ nicht Null ist, sind die Vektoren q_1, p_1 und u_1 nach 1.11 linear abhängig. Wäre $u_1 = p_1k$ mit einem $k \in K$, so folgte

$$0 = q_1 \otimes (q_2 \otimes (q_2 \otimes \cdots \otimes q_t) + p_1 \otimes (y + (p_2 \otimes \cdots \otimes p_t)k)$$

im Widerspruch zur linearen Unabhängigkeit von q_1 und p_1. Somit sind u_1 und p_1 linear unabhängig. Es gibt daher $a, b \in K$ mit $q_1 = u_1 a + p_1 b$. Es folgt $a \neq 0$ und

$$0 = u_1 \otimes ((q_2 \otimes \cdots \otimes q_t)a + p_2 \otimes \cdots \otimes p_t) + p_1 \otimes z$$

mit einem geeigneten z. Weil u_1 und p_1 linear unabhängig sind, folgt

$$0 = (q_2 \otimes \cdots \otimes q_t)a + p_2 \otimes \cdots \otimes p_t.$$

Hieraus folgt nun mittels Induktion, dass $q_i \in p_i K$ ist für $i := 2, \ldots, t$. Dies zeigt, dass $Q \leq U_1(P)$ ist.

Es seien Q und R zwei Punkte von U, die beide von P verschieden seien. Es gibt dann i und j mit $Q \leq U_i(P)$ und $R \leq U_j(P)$, wie wir gerade gesehen hatten. Wir zeigen, dass $i = j$ ist. Dazu nehmen wir an, dass dies nicht der Fall sei. Wir dürfen dann annehmen, dass $i = 1$ und $j = 2$ ist. Es folgt $Q = (u_1 \otimes p_2 \otimes \cdots \otimes p_t)K$ und $R = (p_1 \otimes u_2 \otimes \cdots \otimes p_t)K$ mit $u_i \in V_i$ für $i := 1, 2$. Es folgt, dass auch der durch

$$T := (u_1 \otimes p_2 \otimes \cdots \otimes p_t + p_1 \otimes u_2 \otimes \cdots \otimes p_t)K$$

definierte Punkt T ein Punkt auf $S(V_1, \ldots, V_t)$ ist. Es gibt daher ein k mit $T \leq U_k(P)$. Wegen $Q + R = R + T = T + Q$ und $U_1(P) \cap U_2(P) = P$ (Satz 3.4) ist $k \neq 1, 2$. Daher dürfen wir annehmen, dass $k = 3$ ist. Es folgt $T = (p_1 \otimes p_2 \otimes u_3 \otimes \cdots p_t)K$ mit $u_3 \in V_3$, so dass es ein $k \in K$ gibt mit

$$(u_1 \otimes p_2 \otimes p_3 + p_1 \otimes u_2 \otimes p_3 + p_1 \otimes p_2 \otimes u_3 k) \otimes \cdots \otimes p_t = 0.$$

Hieraus folgt

$$u_1 \otimes p_2 \otimes p_3 + p_1 \otimes u_2 \otimes p_3 + p_1 \otimes p_2 \otimes u_3 k = 0$$

und weiter

$$u_1 \otimes (p_2 \otimes p_3) + p_1 \otimes (u_2 \otimes p_3 + p_2 \otimes u_3 k) = 0,$$

so dass u_1 und p_1 linear abhängig sind. Dies hat aber $Q = P$ zur Folge. Damit ist gezeigt, dass es ein i gibt, so dass alle von P verschiedenen Punkte von U in $U_i(P)$ liegen. Also ist $U \leq U_i(P)$.

3.7. Satz. *Es sei K ein kommutativer Körper und $V_1, \ldots, V_t$ seien Vektorräume über K. Sind P und Q Punkte auf $S(V_1, \ldots, V_t)$ und ist $U_i(P) \cap U_i(Q) \neq \{0\}$, so ist $U_i(P) = U_i(Q)$.*

Beweis. Es sei $P = (p_1 \otimes \cdots \otimes p_t)K$ und $Q = (q_1 \otimes \cdots \otimes q_t)K$. Auf Grund unserer Voraussetzung gibt es $x_i, y_i \in V_i$ mit

$$0 \neq p_1 \otimes \cdots \otimes x_i \otimes \cdots \otimes p_t = q_1 \otimes \cdots \otimes y_i \otimes \cdots \otimes q_t.$$

Hieraus folgt $p_j K = q_i K$ für alle von i verschiedenen j. Dies zeigt, dass $U_i(P) = U_i(Q)$ ist.

Besonders einfach sind Segresche Mannigfaltigkeiten mit nur zwei Parameterräumen. Für diese gilt der folgende Satz, der uns sogleich von Nutzen sein wird.

3.8. Satz. *Es sei K ein kommutativer Körper und V_1 und V_2 seien Vektorräume über K. Sind P und Q zwei Punkte von $S(V_1, V_2)$, so ist $U_1(P) \cap U_2(Q)$ ein Punkt.*

Beweis. Es sei $U_1(P) = \{x_1 \otimes p_2 \mid x_1 \in V_1\}$ und $U_2(Q) = \{q_1 \otimes x_2 \mid x_2 \in V_2\}$. Setze $R := (p_1 \otimes q_2)K$. Dann ist R ein Punkt mit $R \leq U_1(P) \cap U_2(Q)$. Mit 3.7 und 3.4 folgt

$$U_1(P) \cap U_2(Q) = U_1(R) \cap U_2(R) = R.$$

Damit ist der Satz bewiesen.

3.9. Satz. *Es sei K ein kommutativer Körper und $V_1, \ldots, V_t$ seien Vektorräume über K. Ist U ein Teilraum von $\bigotimes_{i:=1}^t V_i$ und liegen alle Punkte von U auf $S(V_1, \ldots, V_t)$, so gibt es einen Punkt P auf $S(V_1, \ldots, V_t)$ und ein i mit $U \leq U_i(P)$.*

Beweis. Wir machen Induktion nach t. Sei also zunächst $t = 2$. Ferner seien Q und R zwei verschiedene Punkte auf U. Setze $P := U_1(Q) \cap U_2(R)$. Nach 3.8 ist P ein Punkt. Mit 3.7 folgt weiter $U_1(Q) = U_1(P)$ und $U_2(R) = U_2(P)$. Daher ist

$$Q + R \leq T(P).$$

Weil alle Punkte von $Q + R$ zu $S(V_1, V_2)$ gehören, folgt nach 3.6 dass es ein $i \in \{1, 2\}$ gibt mit

$$Q + R \leq U_i(P).$$

Hieraus folgt $U_i(Q) = U_i(R)$. Es sei S ein von Q und R verschiedener Punkt von U. Dann folgt mit dem gleichen Argument, dass es $k, l \in \{1, 2\}$ gibt mit $U_k(Q) = U_k(S)$ und $U_k(S)$ und $U_l(R) = U_l(S)$ ist. Ist $k = 1$, so folgt

$$Q + R \leq U_k(S) \cap U_i(P)$$

und damit $k = i$, da ja $Q + R$ eine Gerade ist. In diesem Falle ist $S \leq U_i(P)$. Ist $k \neq l$, so ist, da wir nur zwei Indizes zur Auswahl haben, $k = i$ oder $l = i$, so dass auch hier $S \leq U_i(P)$ gilt. Weil U die obere Grenze der in U enthaltenen Punkte ist, ist daher $U \leq U_i(P)$.

Es sei nun $t > 2$. In diesem Falle identifizieren wir $\otimes_{i:=1}^t V_i$ mit $(\otimes_{i:=1}^{t-1} V_i) \otimes V_t$. Dann liegen die Punkte von U alle auf

$$S\Big(\bigotimes_{i:=1}^{t-1} V_i, V_t\Big).$$

Nach dem bereits Bewiesenen liegen die Punkte von U entweder in einem Teilraum der Form

$$\{v \bigotimes x_t \mid x_t \in V_t\}$$

mit einem $v \in \bigotimes_{i:=1}^{t-1} V_i$ oder in einem Teilraum der Form

$$\{y \otimes v_t \mid y \in \bigotimes_{i:=1}^{t-1} V_i\}$$

mit einem $v_t \in V_t$. Im ersten Falle folgt, weil die Punkte von U ja in der Segreschen Mannigfaltigkeit liegen, dass v zerlegbar ist. Das bedeutet aber, dass es einen Punkt P auf der Segreschen Mannigfaltigkeit gibt mit $U \leq U_t(P)$. Im zweiten Falle folgt aus der Induktionsannahme, dass es einen Punkt P sowie ein i gibt mit $1 \leq i \leq t-1$ und $U \leq U_i(P)$. Damit ist auch dieser Satz bewiesen.

Die Räume $U_i(P)$ spielen eine hervorragende Rolle, wie wir jetzt schon sehen. Daher setzen wir

$$E_i := \{U_i(P) \mid P \in S(V_1, \ldots, V_t)\}$$

und nennen E_i die $i$te *Schar von Erzeugenden* von $S(V_1, \ldots, V_t)$. Ist $t = 2$ und $\mathrm{Rg}_K(V_i) = 2$ für beide i, so heißen E_1 und E_2 auch *Regelscharen* bzw. *reguli* (Einzahl: *regulus*. Blaschke bildet den Plural „Regulusse".) Völlig unklar ist mir die Herkunft von *regulus*. Im Lateinischen bedeutet es „König eines kleinen Landes", weiter einen kleinen Vogel, hinter dem man den Zaunkönig vermutet und, als Übersetzung von $\beta\alpha\sigma\iota\lambda\iota\sigma\kappa o\varsigma$, „Basilisk", eine Eidechsenart. Ich weiß auch nicht, welches der beiden Wörter „Regelschar" und *regulus* im Sinne von Regelschar älter ist.

3.10. Satz. *Es seien V_1 und V_2 Vektorräume über dem kommutativen Körper K. Sind $x, y, z \in V_1$ und $u, v, w \in V_2$ und gilt $x \otimes u + y \otimes v = z \otimes w$, so sind x und y oder u und v linear abhängig.*

Beweis. Die Vektoren x und y seien linear unabhängig. Ist $u = 0$ oder $v = 0$, so ist nichts zu beweisen. Es sei also $u \neq 0$ und $v \neq 0$. Es sei ferner B eine Basis von V_1 mit $x, y \in B$ und C sei eine Basis von V_2. Schließlich sei $z = \sum_{b \in B} b\zeta_b, u = \sum_{c \in C} c\alpha_c, v = \sum_{c \in C} c\beta_c$ und $w = \sum_{c \in C} c\gamma_c$. Dann ist

$$\sum_{c \in C}(x \otimes c)\alpha_c + \sum_{c \in C}(y \otimes c)\beta_c = \sum_{b \in B}\sum_{c \in C}(b \otimes c)\zeta_b\gamma_c.$$

Da die $b \otimes c$ eine Basis von $V_1 \otimes_K V_2$ bilden, folgt $\alpha_c = \zeta_x\gamma_c$ und $\beta_c = \zeta_y\gamma_c$ für alle $c \in C$. Hieraus folgt $u = w\zeta_x$ und $v = w\zeta_y$. Weil u und v nicht Null sind, sind ζ_x und ζ_y nicht Null, so dass u und v in der Tat linear abhängig sind.

Ich weiß nicht, ob man beim nächsten Satz auf die Voraussetzung der Endlichkeit der Ränge verzichten kann.

3.11. Satz. *Es sei K ein kommutativer Körper und $V_1, \ldots, V_t$ seien Vektorräume über K mit $2 \leq \mathrm{Rg}_K(V_i) < \infty$. Ist $\sigma \in GL(\bigoplus_{i:=1}^{t} V_i)$ und gilt*

$$S(V_1, \ldots, V_t)^\sigma = S(V_1, \ldots, V_t),$$

so gibt es ein $\pi \in S_t$ mit $E_i^\sigma = E_{\pi(i)}$ für $i := 1, \ldots, t$.

Beweis. Wegen 3.3 dürfen wir annehmen, dass

$$2 \leq \mathrm{Rg}_K(V_1) \leq \ldots \leq \mathrm{Rg}_K(V_t)$$

ist.

Es sei U ein Element von E_t. Da die Segresche Mannigfaltigkeit $S(V_1, \ldots, V_t)$ invariant unter σ ist, liegen alle Punkte von U^σ auf $S(V_1, \ldots, V_t)$. Nach 3.9 gibt es daher ein j und ein $W \in E_j$ mit $U^\sigma \leq W$. Auf Grund unserer Annahme über die Ränge der V_i folgt $U^\sigma = W$. Wir wollen zeigen, dass hieraus folgt, dass $E_t^\sigma = E_j$ ist. Dazu dürfen wir wegen 3.3 annehmen, dass $j = t$ ist.

Es ist

$$U = \{p_1 \otimes \cdots \otimes p_{t-1} \otimes x \mid x \in V_t\}$$

und

$$U^\sigma = \{q_1 \otimes \cdots \otimes q_{t-1} \otimes y \mid y \in V_t\}.$$

Es sei $W := \{w_1 \otimes p_2 \cdots \otimes p_{t-1} \otimes x \mid x \in V_t\}$, aber $W^\sigma \notin E_t$. Wir können annehmen, dass $W^\sigma \in E_{t-1}$ ist. Es gibt dann Vektoren r_i mit

$$W^\sigma = \{r_1 \otimes \cdots \otimes r_{t-2} \otimes x \otimes r_t \mid x \in V_{t-1}\}.$$

Weil der Rang von V_t mindestens 2 ist, gibt es ein $y \in V_t$, so dass y und r_t linear unabhängig sind. Es gibt ferner ein $x \in V_t$ mit

$$(p_1 \otimes \cdots \otimes p_{t-1} \otimes x)^\sigma = q_1 \otimes \cdots \otimes q_{t-1} \otimes y$$

und ein $z \in V_{t-1}$ mit

$$(w_1 \otimes p_2 \otimes \cdots \otimes p_{t-1} \otimes x)^\sigma = r_1 \otimes \cdots \otimes r_{t-2} \otimes z \otimes r_t.$$

Nun ist

$$q_1 \otimes \cdots \otimes q_{t-1} \otimes y + r_1 \otimes \cdots \otimes r_{t-2} \otimes z \otimes r_t = ((p_1 + w_1) \otimes p_2 \otimes \cdots p_{t-1} \otimes x)^\sigma$$

Weil σ zerlegbare Tensoren auf zerlegbare Tensoren abbildet und weil y und r_n linear unabhängig sind, folgt mit 3.10, dass es ein $k \in K$ gibt mit

$$q_1 \otimes \cdots \otimes q_{t-1} = (r_1 \otimes \ldots \otimes r_{t-2} \otimes z)k.$$

Hieraus folgt $q_i K = r_i K$ für $i := 1, \ldots, t-2$ und $q_{t-1}K = zK$. Dies impliziert die Existenz eines $l \in K$ mit

$$q_1 \otimes \cdots q_{t-1} \otimes y + r_1 \otimes \cdots \otimes r_{t-2} \otimes z \otimes r_t = q_1 \otimes \cdots \otimes q_{t-1} \otimes (q + r_t l).$$

Also ist

$$((p_1 + w_1) \otimes p_2 \otimes \cdots \otimes p_{t-1} \otimes x)^\sigma = q_1 \otimes \cdots \otimes q_{t-1} \otimes (y + r_t l).$$

Der letzte Vektor liegt aber im Bild von U unter σ. Es gibt also ein $u \in V_t$ mit

$$p_1 \otimes \cdots \otimes p_{t-1} \otimes u = (p_1 + w_1) \otimes p_2 \otimes \cdots \otimes p_{t-1} \otimes x.$$

Hieraus folgt schließlich, dass p_1 und w_1 linear abhängig sind, so dass $U = W$ ist. Dieser Widerspruch zeigt, dass doch $W^\sigma \in E_t$ ist.

Ist $i \geq 1$ und ist bereits gezeigt, dass

$$\{w_1 \otimes \cdots \otimes w_i \otimes p_{i+1} \otimes \cdots \otimes p_{t-1} \otimes x \mid x \in V_t\}^\sigma$$

in E_t liegt, so folgt mittels 3.3 und dem bereits Bewiesenen, dass auch

$$\{w_1 \otimes \cdots \otimes w_{i+1} \otimes p_{i+2} \otimes \cdots \otimes p_{t-1} \otimes x \mid x \in V_t\}^\sigma$$

in E_t liegt. Damit ist gezeigt, dass $E_t^\sigma = E_t$ ist.

Die Behauptung des Satzes folgt nun mittels Induktion nach t.

Wir sind nun in der Lage, den Stabilisator $\hat{G}(V_1, \ldots, V_t)$ von $S(V_1, \ldots, V_t)$ in $PGL(\bigotimes_{i:=1}^t V_i)$ zu bestimmen.

3.12. Satz. *Es sei K ein kommutativer Körper und $V_1, \ldots, V_t$ seien Vektorräume endlichen Ranges über K mit $2 \leq \mathrm{Rg}_K(V_i)$ für alle i. Ist σ eine Kollineation von $\mathrm{L}_K(\bigotimes_{i:=1}^t V_i)$, die $S(V_1, \ldots, V_t)$ invariant lässt, und gibt es einen Punkt $P \in S(V_1, \ldots, V_t)$, so dass σ den Tangentialraum $T(P)$ punktweise festlässt, so ist $\sigma = 1$.*

Beweis. Weil der Rang von $T(P)$ mindestens 2 ist, wird σ durch eine lineare Abbildung induziert. Dies werden wir später verwenden.

Eine zweite Bemerkung, die uns gleich nützlich sein wird, ist die, dass $S(V_1, \ldots, V_t)$ einen Rahmen von $\bigotimes_{i:=1}^t V_i$ enthält, woraus nach III.1.10 folgt, dass einzig die Identität unter den projektiven Kollineationen $S(V_1, \ldots, V_t)$ punktweise festlässt. Um die Existenz des Rahmens zu zeigen, sei B_i eine Basis von V_i. Setzt man $u_i := \sum_{b \in B_i} b$, und definiert man b_α durch $b_\alpha := \alpha(1) \otimes \cdots \otimes \alpha(t)$ für alle $\alpha \in \mathrm{cart}_{i:=1}^t B_i$, so bilden die Punkte $P_0 := (u_1 \otimes \cdots \otimes u_t)K, P_\alpha := b_\alpha K$ einen Rahmen von $\bigotimes_{i:=1}^t V_i$.

Es sei $t = 2$. Ferner sei Q ein Punkt von $S(V_1, V_2)$. Dann ist $R := U_1(Q) \cap U_2(P)$ nach 3.8 ein Punkt. Es folgt $U_1(Q) = U_1(R)$ und $U_2(P) = U_2(R)$. Es folgt, dass R und $U_2(R)$ unter σ festbleiben. Dann bleibt aber auch $U_1(R)$ unter σ fest. Wegen $U_1(R) = U_1(Q)$ ist also $U_1(Q)$ unter σ fest. Genauso zeigt man, dass auch $U_2(Q)$ unter σ festbleibt. Wegen $Q = U_1(Q) \cap U_2(Q)$ ist folglich Q bei σ fest. Dies zeigt, dass σ alle Punkte von $S(V_1, V_2)$ festlässt. Weil σ von einer linearen Abbildung induziert wird, ist σ nach obiger Bemerkung die Identität.

Es sei nun $t > 2$ und $P = (p_1 \otimes \cdots \otimes p_t)K$. Ist $0 \neq x_t \in V_t$, so ist $X := (p_1 \otimes \cdots \otimes p_{t-1} \otimes x_t)K$ ein Punkt von $U_t(P)$. Hieraus folgt $X^\sigma = X$. Dies impliziert, dass $U_{t-1}(X)^\sigma = U_{t-1}(X)$ ist. Da dies für jedes x_t gilt, folgt, dass der Raum W, der von

$$\{p_1 \otimes \cdots \otimes p_{t-2} \otimes x_{t-1} \otimes x_t \mid x_{t-1} \in V_{t-1}, x_t \in V_t\}$$

erzeugt wird, unter σ invariant ist. Die Punkte von $S(V_1, \ldots, V_t)$, die in W liegen, bilden eine zu $S(V_{t-1}, V_t)$ isomorphe Segremannigfaltigkeit. Da P zu dieser Mannigfaltigkeit gehört und da der Tangentialraum $U_{t-1}(P) + U_t(P)$ an

diese Mannigfaltigkeit im Punkte P als Unterraum von $T(P)$ ebenfalls punktweise festbleibt, folgt, dass W von σ punktweise festgelassen wird. Nun ist $\bigotimes_{i:=1}^{t} V_i$ zu

$$\left(\bigotimes_{i:=1}^{t-2} V_i\right) \otimes (V_{t-1} \otimes V_t)$$

in kanonischer Weise isomorph, so dass wir diese beiden Vektorräume identifizieren dürfen. Dann lässt aber σ die Räume $\sum_{i:=1}^{t-2} U_i(P)$ und W punktweise fest. Die lineare Abbildung, von der σ induziert wird, wirkt auf diesen beiden Räumen als Skalarmultiplikation. Da P im Durchschnitt dieser beiden Räume liegt, wird sie auf beiden Räumen durch die gleiche Skalarmultiplikation dargestellt. Somit lässt σ den Tangentialraum $T'(P)$ von $S(V_1, \ldots, V_{t-2}, V_{t-1} \otimes V_t)$ punktweise fest. Nach Induktionsannahme ist daher $\sigma = 1$.

3.13. Satz. *Es sei K ein kommutativer Körper und $V_1, \ldots, V_t$ seien Vektorräume endlichen Ranges über K. Es sei*

$$\{r_1, \ldots, r_s\} := \{\mathrm{Rg}_K(V_i) \mid i := 1, \ldots, t\}$$

und

$$2 \leq r_1 < r_2 < \ldots < r_s.$$

Ferner sei α_j die Anzahl der i mit $\mathrm{Rg}_K(V_i) = r_j$. Ist $G(V_1, \ldots, V_t)$ diejenige Untergruppe von $\hat{G}(V_1, \ldots, V_t)$, die die Erzeugendenscharen E_i von $S(V_1, \ldots, V_t)$ jede für sich invariant lässt, so ist

$$\hat{G}(V_1, \ldots, V_t)/G(V_1, \ldots, V_t) \cong S_{\alpha_1} \times \cdots \times S_{\alpha}$$

und

$$G(V_1, \ldots, V_t) \cong PGL(V_1) \times \cdots \times PGL(V_t).$$

Beweis. Die erste Aussage folgt unmittelbar aus 3.11.

Es sei $\rho_i \in GL(V_i)$ für $i := 1, \ldots, t$. Mit Hilfe von 3.2 und 1.3 erhalten wir die Existenz genau einer Abbildung $\rho_1 \otimes \cdots \otimes \rho_t$ mit

$$(v_1 \otimes \cdots \otimes v_t)^{\rho_1 \otimes \cdots \otimes \rho_t} = v_1^{\rho_1} \otimes \cdots \otimes v_t^{\rho_t}.$$

Es sei η die Abbildung, die dem Element $(\rho_1, \ldots, \rho_t)$ die von $\rho_1 \otimes \cdots \rho_t$ in $\mathrm{L}_K(\bigotimes_{i:=1}^{t} V_i)$ induzierte Kollineation zuordnet. Dann ist η ein Homomorphismus von $GL(V_1) \times \cdots \times GL(V_t)$ in $G(V_1, \ldots, V_t)$. Es sei $(\rho_1, \ldots, \rho_t)$ im Kern von η. Es gibt dann ein $k \in K^*$ mit

$$v_1^{\rho_1} \otimes \cdots \otimes v_t^{\rho_t} = (v_1 \otimes \cdots \otimes v_t)k.$$

Hieraus folgt die Existenz von $k_i \in K^*$ mit $v_i^{\rho_i} = v_i k_i$ für $i := 1, \ldots, t$. Dies zeigt, dass η einen Monomorphismus von $PGL(V_1) \times \cdots \times PGL(V_t)$ in $G(V_1, \ldots, V_t)$ induziert.

Es bleibt zu zeigen, dass η surjektiv ist. Dazu sei σ eine lineare Abbildung, die eine Kollineation aus $G(V_1, \ldots, V_t)$ induziert. Es sei $P = (p_1 \otimes \cdots \otimes p_t)K$

ein Punkt von $S(V_1, \ldots, V_t)$. Dann ist auch P^σ ein Punkt von $S(V_1, \ldots, V_t)$. Es gibt folglich $Q_i \in V_i$ mit

$$(p_1 \otimes \ldots, \otimes p_t)^\sigma = q_1 \otimes \ldots \otimes q_t.$$

Es gilt dann $U_i(P)^\sigma = U_i(P^\sigma)$ für alle i. Es gibt daher eine Abbildung $\sigma_i \in GL(V_i)$ mit

$$(p_1 \otimes \cdots \otimes x_i \otimes \cdots \otimes p_t)^\sigma = q_1 \otimes \cdots \otimes x_i^{\sigma_i} \otimes \cdots \otimes q_t$$

und es folgt $p_i^{\sigma_i} = q_i$. Nach dem, was wir bereits gezeigt haben, induziert $\sigma(\sigma_1 \otimes \cdots \otimes \sigma_t)^{-1}$ eine Kollineation, die zu $G(V_1, \ldots, V_t)$ gehört. Diese Kollineation lässt aber $T(P)$ punktweise fest, da die lineare Abbildung $\sigma(\sigma_1 \otimes \cdots \otimes \sigma_t)^{-1}$ die Unterräume $U_i(P)$ vektorweise festlässt. Mit 3.12 folgt daher, dass die fragliche Kollineation die Identität ist. Also ist $\sigma = \sigma_1 \otimes \cdots \otimes \sigma_t$, so dass η auch surjektiv ist. Damit ist alles bewiesen.

4. Geometrische Erzeugung Segrescher Mannigfaltigkeiten

Die Definition der Segreschen Mannigfaltigkeiten, die wir im letzten Abschnitt gegeben haben, lässt natürlich viel zu wünschen übrig. Sie gibt eine rein algebraische Beschreibung dieser Objekte, so dass sich die Frage erhebt, ob es geometrische Kennzeichnungen dieser Mannigfaltigkeiten gibt. Die Antwort lautet natürlich „ja“, zumindest, wenn wir die Endlichkeit der Ränge der Parameterräume voraussetzen.

4.1. Satz. *Es sei L ein projektiver Verband und $U_1, \ldots, U_n$ seien unabhängige Elemente dieses Verbandes, dh., es gelte*

$$U_k \cap \sum_{i \in X} U_i = 0$$

für alle echten Teilmengen X von $\{1, \ldots, n\}$ und alle Indizes k, die nicht in X liegend. Ist P ein Punkt von $\sum_{i:=1}^n U_i$ und gilt

$$P \not\leq \sum_{i \in X} U_i$$

für alle echten Teilmengen X von $\{1, \ldots, n\}$, so gibt es genau einen Teilraum T des Ranges n von L, der P enthält und der jeden der Räume U_i nicht trivial schneidet.

Es ist $T \cap U_i$ für alle i ein Punkt und $\{T \cap U_i \mid i := 1, \ldots, n\}$ ist eine Basis von T.

Beweis. Wir machen Induktion nach n. Es sei zunächst $n = 2$. In diesem Falle setzen wir

$$T := (U_1 + P) \cap (U_2 + P).$$

Dann ist $P \leq T$. Auf Grund des Modulargesetzes gilt

$$U_1 + ((U_1 + P) \cap U_2) = (U_1 + P) \cap (U_1 + U_2) = U_1 + P,$$

da ja $P \leq U_1 + U_2$ ist. Hieraus folgt, dass $(U_1 + P) \cap U_2$ ein Punkt ist, da P ja nicht in U_1 liegt. Wegen

$$T \cap U_2 = (U_1 + P) \cap (U_2 +)) \cap U_2 = (U_1 + P) \cap U_2$$

ist $T \cap U_2$ also ein Punkt. Ebenso sieht man, dass $T \cap U_1$ ein Punkt ist. Nochmalige Benutzung des Modulargesetzes liefert

$$T = (U_1 + P) \cap (P + U_2) = P + ((U_1 + P) \cap U_2),$$

so dass T die Summe zweier Punkte ist. Folglich ist T eine Gerade. Damit ist die Existenz von T gezeigt. Ist andererseits T' eine Gerade durch P, die U_1 und U_2 trifft, so ist

$$T' \leq (U_1 + P) \cap (U_2 + P) = T,$$

womit auch die Einzigkeit von T nachgewiesen ist.

Es sei nun $n \neq 3$. Wir setzen $V := \sum_{i:=1}^{n-1} U_i$. Dann gilt $P \leq V + U_n$ und $P \not\leq V, U_n$. Nach dem bereits Bewiesenen gibt es genau eine Gerade G durch P, die V und U_n jeweils in einem Punkte trifft. Setze $Q := V \cap G$. Ist dann X eine echte Teilmenge von $\{1, \ldots, n-1\}$, so folgt $Q \not\leq \sum_{i \in U_i}$, da andernfalls $P \leq \sum_{i \in X \cup \{n\}} U_i$ wäre. Es gibt also einen Teilraum H des Ranges $n-1$, der durch Q geht und jeden der Teilräume U_i mit $i < n$ nicht trivial trifft. Setzt man $T := G + H$, so liegt P auf T und T schneidet jeden der Räume U_i nicht trivial. Nun ist offenbar $G \cap H = Q$ und daher

$$\mathrm{Rg}_L(T) = \mathrm{Rg}_L(G) + \mathrm{Rg}_L(H) - 1 = 2 + n - 1 - 1 = n,$$

so dass die Existenz von T bewiesen ist.

Die Bedeutungen von G, H, Q und V werden beibehalten. Es sei T' ein Raum des Ranges n, der P enthält und alle U_i nicht trivial schneidet. Weil die U_i unabhängig sind, folgt

$$n \geq \mathrm{Rg}_L\biggl(\sum_{i:=1}^{n} (U_i \cap T')\biggr) = \sum_{i:=1}^{n} \mathrm{Rg}_L(U_i \cap T') \geq n$$

und weiter $\mathrm{Rg}_L(U_i \cap T') = 1$. Setze $R_i := U_i \cap T'$. Dann ist $R_n \leq P + U_n$. Wegen $P \not\leq \sum_{i:=1}^{n-1} R_i$ ist $T' = P + \sum_{i:=1}^{n-1} R_i$. Es folgt $R_n \leq P + V$. Dies besagt, dass $R_n \leq (P + U_n) \cap (P + V) = G$ ist. Also ist $G \leq T'$. Es folgt, dass auch $Q \leq T'$ ist. Also ist $T' \cap V$ ein Raum des Ranges $n-1$ durch Q, der die U_i mit $i \leq n-1$ nicht trivial schneidet. Nach Induktionsannahme ist daher $T' \cap V = H$ und weiter $T = T'$. Damit ist die Einzigkeit von T bewiesen. Gleichzeitig sehen wir, dass $T \cap U_i$ ein Punkt ist und dass die Menge dieser Punkte eine Basis von T ist. Damit ist alles bewiesen.

Da T die Räume U_i *transversal* schneidet, nennen wir T *Transversale* der U_i durch den Punkt P.

4.2. Satz. *Es sei L ein projektiver Verband endlichen Ranges mit dem größten Element* Π. *Ferner seien $U_1, \ldots, U_n, D \in L$ und* Π *sei die direkte Summe von*

je n von ihnen. Ist P ein Punkt auf D, so bezeichne T_P die Transversale der $U_1, \ldots, U_n$ durch den Punkt P. Es gilt nun:
a) *Ist B eine Basis von D, so ist*

$$B_i := \{T_P \cap U_i \mid P \in B\}$$

eine Basis von U_i.
b) *Ist C ein Rahmen von D, so ist*

$$C_i := \{T_P \cap U_i \mid P \in C\}$$

eine Rahmen von U_i.
c) *Ist B eine Basis von D und ist $P \in B$, so ist*

$$\{P\} \cup \{T_P \cap U_i \mid i := 1, \ldots, n\}$$

ein Rahmen von T_P.

Beweis. a) Wir setzen $V_i = \sum_{P \in B_i} P$. Dann ist $V_i \leq U_i$. Es folgt

$$T_P \leq U_1 + \ldots + U_{i-1} + V_i + U_{i+1} + \ldots + U_n.$$

Wegen $P \leq T_P$ ist also

$$D \leq U_1 + \ldots + U_{i-1} + V_i + U_{i+1} + \ldots + U_n.$$

Dann ist aber

$$\begin{aligned} \Pi &= U_1 + \ldots + U_{i-1} + D + U_{i+1} + \ldots + U_n \\ &\leq U_1 + \ldots + U_{i-1} + V_i U_{i+1} + \ldots + U_n, \end{aligned}$$

so dass wegen der Unabhängigkeit der U_j folgt, dass $U_i = V_i$ ist. Somit ist B_i ein Erzeugendensystem von U_i. Weil Π von je n der Räume $U_1, \ldots, U_n, D$ erzeugt wird, sind diese Räume alle isomorph. Daher ist B_i ein minimales Erzeugendensystem, dh., eine Basis von U_i.

b) folgt unmittelbar aus a).

c) folgt mit 4.1.

4.3. Korollar. *Es sei K ein Körper und V sei ein Vektorraum endlichen Ranges über K. Ferner seien $U_1, \ldots, U_n, D \in \mathrm{L}_K(V)$ und V sei die direkte Summe von je n dieser Räume. Ebenso sei V die direkte Summe von je n der $U_1', \ldots, U_n', \ldots, U_n', D' \in \mathrm{L}_K(V)$. Ist dann $P_0, \ldots, P_r$ ein Rahmen von D und $P_0', \ldots, P_r'$ ein Rahmen von D', so gibt es ein $\sigma \in PGL(V)$ mit*

$$U_i^\sigma = U_i'$$

für $i := 1, \ldots, n$ und

$$P_j^\sigma = P_j'$$

für $j := 0, \ldots, r$.

Dieses Korollar zu beweisen, sei dem Leser als Übungsaufgabe überlassen.

Unsere bisherige Definition der Segreschen Mannigfaltigkeiten machte explizit Gebrauch von den Parameterräumen $V_1, \ldots, V_t$. Davon wollen wir nun loskommen. Dazu definieren wir jetzt allgemeiner: Es sei W ein Vektorraum endlichen Ranges über dem kommutativen Körper K und S sei eine Menge von Punkten von $\mathrm{L}_K(W)$. Wir nennen S eine *Segremannigfaltigkeit*, falls es K-Vektorräume $V_1, \ldots, V_t$ gibt und einen Isomorphismus σ von $\mathrm{L}_K(\bigotimes_{i:=1}^t V_i)$ auf $\mathrm{L}_K(W)$ mit $S(V_1, \ldots, V_t)^\sigma = S$. Geometrisch relevant ist nur der Fall, dass $t \geq 2$ ist und die Ränge der V_i allesamt ebenfalls mindestens gleich 2 sind. Dann ist der Rang von W mindestens gleich 4, so dass es nach dem zweiten Struktursatz eine semilineare Abbildung von $\bigotimes_{i:=1}^t V_t$ gibt, durch die σ induziert wird. Man sieht leicht, dass es dann auch eine lineare Abbildung von $\bigotimes_{i:=1}^t V_i$ auf W gibt, die einen Isomorphismus der Verbände induziert, welcher $S(V_1, \ldots, V_t)$ auf S abbildet. Da die Ränge der V_i den Isomorphietyp von S völlig festlegen, sagen wir auch, falls es die Deutlichkeit erfordert, dass S eine Segresche Mannigfaltigkeit mit den *Invarianten* $n_1, \ldots, n_t$ sei. Diese Definition ist sorgfältig zu lesen. Sie beinhaltet nämlich auch, dass $\mathrm{Rg}_K(W) = \Pi_{i:=1}^t n_i$ ist, wenn es in $\mathrm{L}_K(W)$ eine Segresche Mannigfaltigkeit mit den Invarianten $n_1, \ldots, n_t$ gibt.

Der nächste Satz zeigt uns, wie man Segresche Mannigfaltigkeiten geometrisch erzeugen kann.

4.4. Satz. *Es seien $n_1, \ldots, n_t$ natürliche Zahlen mit $n_i \geq 2$ für alle i. Es sei K ein kommutativer Körper und W sei ein K-Vektorraum. Schließlich seien $W_1, \ldots, W_{n_t}, D$ Unterräume von W, so dass W die direkte Summe von je n_t von ihnen ist. Ist dann S eine Segresche Mannigfaltigkeit mit den Invarianten $n_1, \ldots, n_{t-1}$ von $\mathrm{L}(D)$ und ist S die Menge der Punkte P von $\mathrm{L}_K(W)$, zu denen es einen Punkt $Q \in S$ gibt, so dass P auf der Transversalen T_Q von $W_1, \ldots, W_{n_t}$ durch Q liegt, so ist $\hat{S}$ eine Segresche Mannigfaltigkeit mit den Invarianten $n_1, \ldots, n_t$.*

Beweis. Es seien $V_1, \ldots, V_t$ Vektorräume über K mit $\mathrm{Rg}_K(V_i) = n_i$. Diese werden wir gleich benutzen.

Aus der Annahme, dass W die direkte Summe von je n_t der Räume $W_1, \ldots,$ W_{n_t}, D ist, folgt, dass die W_i allesamt zu D isomorph sind. Hieraus folgt

$$\mathrm{Rg}_K(W) = n_t \mathrm{Rg}_K(D) = \prod_{i:=1}^t n_i,$$

so dass W als Vektorraum zu $\bigotimes_{i:=1}^t V_i$ isomorph ist. Wir dürfen daher $W = \bigotimes_{i:=1}^t V_i$ annehmen.

Es sei B_i eine Basis von V_i und $A := \mathrm{cart}_{i:=1}^t B_i$. Ferner sei $w_i := \sum_{b \in B_i} b$ und $b_\alpha := \alpha(1) \otimes \cdots \otimes \alpha(t)$ für $\alpha \in A$. Schließlich sei $P_0 := (w_1 \otimes \cdots \otimes w_t)K$ und $P_\alpha := b_\alpha K$. Dann ist

$$\{P_0\} \cup \{P_\alpha \mid \alpha \in A\}$$

ein Rahmen von W, der in $S(V_1, \ldots, V_t)$ enthalten ist, wie wir schon einmal

feststellten. Für $b \in B_t$ setzen wir

$$M_b := \sum_{\alpha \in A, \alpha(t)=b} b_\alpha K$$

und

$$N := \sum_{i:=1,\ldots,t-1, x_i \in V_i} (x_1 \otimes \cdots \otimes x_{t-1} \otimes w_t)K.$$

Alle diese Räume haben den Rang $\prod_{i:=1}^{t-1} n_i$, sind also isomorph zueinander. Ferner folgt, weil $\{b_\alpha \mid \alpha \in A\}$ eine Basis von W ist, dass W die direkte Summe der M_b ist. Es sei $c \in B_t$ und $y \in N \cap \sum_{b \in B_{t-\{c\}}} M_b$. Wegen $y \in N$ ist $y = v \otimes w_t$ mit $v \in \bigotimes_{i:=1}^{t-1} V_i$. Andererseits ist $y = \sum_{\alpha \in A, \alpha(t) \neq c} b_\alpha k_\alpha$. Hieraus folgt mit Umsortieren der Summanden $y = \sum_{b \in B_t - \{c\}} v_b \otimes b$ mit $v_b \in \bigotimes_{i:=1}^{t-1} V_i$. Also ist

$$y = v \otimes w_t = \sum_{b \in B_t - \{c\}} v_b \otimes b.$$

Weil w_t die Summe aller $b \in B_t$ ist, folgt, dass auch $(B_t - \{c\}) \cup \{w_t\}$ eine Basis von V_t ist. Mit 1.11 folgt daher, dass unter anderem $v = 0$ ist. Also ist $y = 0$. Hieraus folgt schließlich, dass W auch die direkte Summe von D und $\sum_{b \in B_{t-\{c\}}} M_b$ ist. Wegen 4.3 dürfen wir also annehmen, dass $D = N$ und dass

$$\{W_i \mid i := 1, \ldots, n_t\} = \{M_b \mid b \in B_t\}$$

ist. Die Untergruppe der projektiven Gruppe, die die Räume N und M_α jeden für sich invariant lässt, induziert nach 4.3 und III.1.11 die $PGL(D)$ in $\mathrm{L}_K(D)$. Daher dürfen wir auch noch annehmen, dass S aus den Punkten der Form $(x_1 \otimes \cdots \otimes x_{t-1} \otimes w_t)K$ besteht. Wir müssen schließlich noch zeigen, dass $\hat{S} = S(V_1, \ldots, V_t)$ ist. Dazu sei $P := (x_1 \otimes \cdots \otimes x_t)K$ ein Punkt von S und es gelte

$$P \leq U_t(Q).$$

Ist $b \in B_t$, so ist $(x_1 \otimes \cdots \otimes x_{t-1} \otimes b)K$ ein Punkt auf $U_t(Q)$, aber auch auf M_b. Dies zeigt, dass $U_t(Q)$ eine Transversale der M_b ist. Also ist $P \in \hat{S}$ und folglich $S(V_1, \ldots, V_t) \subseteq \hat{S}$. Ist andererseits $R \in \hat{S}$, so gibt es einen Punkt $Q \in S$, so dass R auf der Transversalen T_Q der Räume M_b durch den Punkt Q liegt. Wie wir bereits feststellten, ist auch $U_t(Q)$ eine Transversale der M_b durch Q. Nach 4.3 ist daher $T_Q = U_t(Q)$, so dass $P \in S(V_1, \ldots, V_t)$ ist. Damit ist alles bewiesen.

Da $S(V_1)$ nichts anderes als die Menge der Punkte von $\mathrm{L}_K(V_1)$ ist, ist nach diesem Satz klar, wie man sich rekursiv eine Segremannigfaltigkeit mit vorgegebenen Invarianten rein geometrisch konstruieren kann. Besonders zufriedenstellend ist das Verfahren, wenn man eine Segremannigfaltigkeit mit nur zwei Invarianten konstruieren will. Sind beide Invarianten 2, so erhält man eine Segremannigfaltigkeit, die man in der schönen alten Zeit bereits in der Vorlesung „Analytische Geometrie“ unter dem Namen *Hyperboloid* kennenlernte.

4.5. Satz. *Es sei K ein kommutativer Körper und V sei ein Vektorraum des Ranges 4 über K. Ist S eine Segremannigfaltigkeit mit den Invarianten 2, 2 in $\mathrm{L}_K(V)$, so ist S eine Quadrik, die durch eine quadratische Form von maximalen Index dargestellt wird.*

Beweis. Wir können annehmen, dass $V = V_1 \otimes_K V_2$ ist mit zwei Vektorräumen V_i des Ranges 2 über K und dass die fragliche Segremannigfaltigkeit gleich $S(V_1, V_2)$ ist. Es sei b_1, b_2 eine Basis von V_1 und b_3, b_4 eine Basis von V_2 Ist dann $u = b_1k_1 + b_2k_2$ und $v = b_3k_3 + b_4k_4$, so ist

$$u \otimes v = (b_1 \otimes b_3)k_1k_3 + (b_1 \otimes b_4)k_1k_3 + (b_2 \otimes b_3)k_2k_3 + (b_2 \otimes b_4)k_2k_4.$$

Bezeichnet man die Koordinaten eines Vektors bezüglich der Basis aus den $b_i \otimes b_j$ mit x_{ij}, so folgt, dass die Koordinaten des Vektors $u \otimes v$ der quadratischen Gleichung

$$x_{13}x_{24} - x_{14}x_{23} = 0$$

genügen, so dass S also in der durch diese Gleichung definierten Quadrik enthalten ist. Es sei umgekehrt $(x_{13}, x_{14}, x_{23}, x_{24})K$ ein Punkt dieser Quadrik. Da b_1 und b_2 völlig gleichberechtigt sind wie auch b_3 und b_4 und da auch V_1 und V_2 gleiche Rollen spielen, dürfen wir annehmen, dass $x_{13} \neq 0$ ist. Wir setzen

$$k_1 := 1, k_3 := x_{13}, k_2 := \frac{x_{23}}{k_3}, k_4 := x_{14}.$$

Dann ist

$$0 = x_{13}x_{24} - x_{14}x_{23} = k_3x_{24} - k_4k_2k_3.$$

Hieraus folgt $x_{24} = k_2k_4$, da k_3 ja von Null verschieden ist. Dies zeigt, dass alle Punkte der Quadrik zu S gehören. Da durch jeden Punkt von S zwei Geraden gehen, deren Punkte alle zu S gehören, und da diese Geraden nach V.5.4 vollständig isotrop sind, ist der Index der die Quadrik darstellenden quadratischen Form mindestens 2. Weil der Rang von V gleich 4 ist, ist er sogar gleich 2. Damit ist alles gezeigt.

4.6. Satz. *Es sei V ein Vektorraum des Ranges 4 über einem kommutativen Körper. Sind G_1, G_2 und G_3 paarweise windschiefe Geraden von V und ist Q die Menge der Punkte, die auf Transversalen von G_1, G_2 und G_3 liegen, so ist Q eine Quadrik von maximalem Index.*

Beweis. Mittels 4.4 folgt, dass Q eine Segresche Mannigfaltigkeit auf den Invarianten 2, 2 ist. Nach 4.5 ist Q dann eine Quadrik, die durch eine quadratische Form von maximalen Index dargestellt wird.

Wir sind nun in der Lage, Satz I.10.2 zu beweisen, den wir hier noch einmal notieren werden, damit der Leser ihn vor Augen hat.

I.10.2. Satz. *Es sei L ein irreduzibler projektiver Verband, dessen Rang mindestens 4 sei. Genau dann gilt in L der Satz von Pappos, wenn für jedes Hexagramme mystique $G_1, G_2, G_3, H_1, H_2, H_3$ gilt: ist H eine Transversale der G_i und G eine Transversale der H_j, so ist $G \cap H \neq 0$.*

Beweis. Schließt sich jedes Hexagramme mystique, so gilt in L der Satz von Pappos. Dies ist gerade die Aussage des Satzes von Dandelin (Satz I.10.1), den wir nicht noch einmal beweisen werden.

Um die Umkehrung zu beweisen, dürfen wir auf Grund des ersten Struktursatzes annehmen, dass es einen Vektorraum V gibt, so dass $L = \mathrm{L}(V)$ ist. Weil L pappossch ist, ist der Koordinatenkörper von L nach Satz II.6.3 kommutativ. Es sei nun $G_1, G_2, G_3, H_1, H_2, H_3$ ein Hexagramme mystique. Dann ist $U := G_1 + G_2$ ein Unterraum des Ranges 4 und das Hexagramme mystique ist in H enthalten. Wir dürfen daher annehmen, dass $U = V$ ist. Dann ist $\mathrm{Rg}_K(V) = 4$. Nach Satz 4.4 ist die Menge S der Punkte, die auf Transversalen der G_i liegen, eine Segremannigfaltigkeit mit den Invarianten $2, 2$. Dann ist S aber auch die Menge der Punkte, die auf Transversalen der H_i liegen, da durch einen Punkt von H_1 nach Satz 4.1 genau eine Transversale der H_i geht und die Punkte von S alle auf Transversalen der H_i liegen. Ist nun H eine Transversale der G_i und G eine solche der H_i, so folgt mit 3.8, dass $G \cap H$ ein Punkt ist. Damit ist der Beweis von I.10.2 nachgetragen.

Die Segreschen Mannigfaltigkeiten mit den Invarianten $2, 2$ gestatten uns auch eine Frage zu beantworten, die A. F. Möbius im Jahre 1828 im crelleschen Journal stellte und mit Hilfe seines baryzentrischen Kalküls auch sogleich beantwortete, die Frage nämlich: „Kann von zwei dreiseitigen Pyramiden eine jede in Bezug auf die andere um- und einbeschrieben zugleich heissen?“ Solche *Möbiuspaare*, wie sie heute heißen, gibt es in der Tat in jeder dreidimensionalen projektiven Geometrie über einem kommutativen Körper, der wenigstens drei Elemente besitzt.

4.7. Satz. *Es sei K ein kommutativer Körper, der von $GF(2)$ verschieden sei. Es sei ferner V ein Vektorraum des Ranges 4 über K und S sei eine Segresche Mannigfaltigkeit mit den Invarianten $2, 2$ in $\mathrm{L}(V)$ und E_1 und E_2 seien die beiden Geraden aus E_1 und H_1, H_2, H_3, H_4 vier verschiedene Geraden aus E_2. (Damit es solche vier Geraden gibt, braucht man, dass K mindestens drei Elemente enthält.) Setze*

$$
\begin{aligned}
P_0 &:= G_0 \cap H_1 & \qquad Q_0 &:= G_2 \cap H_0 \\
P_1 &:= G_0 \cap H_0 & \qquad Q_1 &:= G_2 \cap H_1 \\
P_2 &:= G_1 \cap H_3 & \qquad Q_2 &:= G_3 \cap H_2 \\
P_3 &:= G_1 \cap H_2 & \qquad Q_3 &:= G_3 \cap H_3.
\end{aligned}
$$

Dann sind die Tetraeder P_0, P_1, P_2, P_3 und Q_0, Q_1, Q_2, Q_3 ein Möbiuspaar.

Beweis. Es ist, da die $G_i \cap H_j$ ja Punkte sind, die für verschiedene Indexpaare auch verschieden sind,

$$
\begin{aligned}
P_0 + P_1 + P_2 &= G_0 \cap H_1 + G_0 \cap H_0 + G_1 \cap H_3 \\
&= G_0 + G_1 \cap H_3 \\
&= G_0 + G_0 \cap H_3 + G_1 \cap H_3 = G_0 + H_3,
\end{aligned}
$$

so dass $Q_3 \leq P_0 + P_1 + P_2$ gilt. Ferner ist

$$\begin{aligned} P_1 + P_2 + P_3 &= G_0 \cap H_0 + G_1 \cap H_3 + G_1 \cap H_2 \\ &= G_0 \cap H_0 + G_1 \\ &= G_0 \cap H_0 + G_1 \cap H_0 + G_1 = H_0 + G_1, \end{aligned}$$

so dass $Q_0 \leq P_1 + P_2 + P_3$ ist. Ganz analog beweist man, dass $Q \leq P_2 + P_3 + P_0$ und $Q_3 \leq P_2 + P_0 + P_1$ gilt.

Ferner gilt

$$\begin{aligned} Q_0 + Q_1 + Q_2 &= H_0 \cap G_2 + H_1 \cap G_2 + H_2 \cap G_3 \\ &= G_2 + H_2 \cap G_2 + H_2 \cap G_3 = G_2 + H_2, \end{aligned}$$

so dass $P_3 \leq Q_0 + Q_1 + Q_2$ ist. Entsprechend beweist man, dass $P_0 \leq Q_1 + Q_2 + Q_3, P_1 \leq Q_2 + Q_3 + Q_0$ ist. Entsprechend beweist man, dass $P_0 \leq Q_1 + Q_2 + Q_3, P_1 \leq Q_2, Q_3 + Q_0$ und $P_2 \leq Q_3 + Q_0 + Q_1$ ist.

Zum Schluß ziehen wir noch eine Folgerung über orthogonale Gruppen aus dem Vorstehenden.

4.8. Satz. *Es sei K ein kommutativer Körper und V sei ein Vektorraum des Ranges 4 über K. Ist Q eine nicht ausgeartete, spurwertige quadratische Form vom Index 2 auf V, so enthält die von $O(V, Q)$ auf $\mathrm{L}(V)$ induzierte Kollineationsgruppe $PO(V, Q)$ einen Normalteiler vom Index 2, welcher zu $PGL(2, K) \times PGL(2, K)$ isomorph ist.*

Beweis. Dies folgt aus der Isometrie der quadratischen Formen von maximalem Index (Satz V.6.6) zusammen mit Satz 4.5 und Satz 3.13.

VII.

Graßmannsche Mannigfaltigkeiten

In diesem Kapitel definieren und studieren wir die graßmannschen Mannigfaltigkeiten eines Vektorraumes. Das sind die Gebilde aus den Unterräumen des Ranges k. Einen sehr wesentlichen Satz über diese Gebilde haben wir schon bewiesen, nämlich den Satz von Chow (Satz I.8.4). Im vorliegenden Kapitel setzen wir nun voraus, dass die Koordinatenkörper kommutativ sind. Das versetzt uns in die Lage, die Unterräume des Ranges k einer projektiven Geometrie des Ranges n durch Punktmannigfaltigkeiten in einem projektiven Raum des Ranges $\binom{n}{k}$ darzustellen. Um dieses Programm durchzuführen, benötigen wir die Graßmannalgebra eines Vektorraumes, die wir mit Hilfe der Tensoralgebra des Vektorraumes definieren werden, so dass wir uns zunächst mit der Tensoralgebra eines Moduls über einem kommutativen Ring beschäftigen werden.

Bei all diesen Untersuchungen ist es ganz wesentlich vorauszusetzen, dass die Moduln Moduln über kommutativen Ringen sind. Ist nämlich M ein Rechtsmodul über einem kommutativen Ring R, so wird M durch die Vorschrift $rm := mr$ für $r \in R$ und $m \in M$ zu einem zweiseitigen R-Modul, für den überdies $rm = mr$ für alle $r \in R$ und alle $m \in M$ gilt. Diese Eigenschaften werden wir ständig auszunutzen haben. Setzt man andererseits voraus, dass M ein zweiseitiger R-Modul ist, für den $rm = mr$ für alle m und r gilt, so folgt mit

$$(rs)m = m(rs) = (mr)s = s(rm) = (sr)m,$$

dass $R/\mathrm{ann}(M)$ kommutativ ist.

1. Die Graßmannalgebra eines Moduls

Im Folgenden sei R ein kommutativer Ring mit Eins. Ist M ein R-Modul, so nehmen wir, wie schon verabredet, an, dass M ein unitärer R-Bimodul sei mit $rm = mr$ für alle $r \in R$ und alle $m \in M$. Wir definieren eine Rekursionsregel ρ durch $\rho(A, M) := A \otimes_R M$ für alle R-Moduln A. Dann ist, wie vor Satz VI.1.9 beschrieben, auch $\rho(A, M)$ ein R-Bimodul. Nach dem Dedekindschen Rekursionssatz gibt es daher eine Abbildung T_R mit $T_R^0(M) = R$ und

$$T_R^{n+1}(M) = T_R^n(M) \otimes_R M.$$

Mittels VI.1.8 und VI.1.7 folgt die Existenz eines Isomorphismus $\sigma_{m,n}$ von $T_R^m(M) \otimes T_R^n(M)$ auf $T_R^{m+n}(M)$ mit

$$\sigma_{m,n}((x_1 \otimes \cdots \otimes x_m) \otimes (y_1 \otimes \cdots \otimes y_n)) = x_1 \otimes \cdots \otimes x_m \otimes y_1 \otimes \cdots \otimes y_n$$

für alle $x_1, \ldots, x_m, y_1, \ldots, y_n \in M$. Dabei ist etwa $x_1 \otimes x_2 \otimes x_3 \otimes x_4$ als $((x_1 \otimes x_2) \otimes x_3) \otimes x_4$ zu lesen. Wir setzen nun

$$T_R(M) := \bigoplus_{i:=0}^{\infty} T_R^i(M).$$

Sind $f, g \in T_R(M)$, so definieren wir fg durch

$$fg := \sum_{n:=0}^{\infty} \sum_{i:=0}^{n} \sigma_{i,n-i}(f_i \otimes g_{n-i}).$$

Dann ist $T_R(M)$ eine R-Algebra mit Eins, die sog. *Tensoralgebra* von M. Die Multiplikation in $T_R(M)$ ist assoziativ.

Wir haben stillschweigend das Element $y \in T_R^i(M)$ mit der Folge aus $T_R(M)$ identifiziert, die an der $i$ten Stelle den Wert y hat und an allen übrigen Stellen Null ist. Diese Identifizierung machen wir nun der Deutlichkeit halber zum Teil wieder rückgängig, indem wir mit $\epsilon(y)$ die Folge f bezeichnen, für die $f_1 = y$ und $f_i = 0$ gilt für alle von 1 verschiedenen i. Dabei ist mit y natürlich ein Element aus $T_R^1(M)$ gemeint.

1.1. Satz. *Es sei R ein kommutativer Ring mit Eins und M sei ein R-Modul und A eine assoziative R-Algebra mit Eins. Ist μ ein Modulhomomorphismus von M in A, so gibt es genau einen Algebrenhomomorphismus α von $T_R(M)$ in A mit $\mu = \alpha\epsilon$.*

Beweis. Auf Grund der Definition der Tensoralgebra ist

$$x_1 \otimes \cdots \otimes x_n = \epsilon(x_1) \ldots \epsilon(x_n)$$

für alle n und alle n-Tupel $(x_1, \ldots, x_n)$ mit $x_i \in M$. Sind α und β nun Algebrenhomomorphismen von $T_R(M)$ in A mit $\alpha\epsilon = \beta\epsilon$, so folgt

$$\begin{aligned}
\alpha(x_1 \otimes \cdots \otimes x_n) &= \alpha(\epsilon(x_1) \ldots \epsilon(x_n)) \\
&= \alpha\epsilon(x_1) \ldots \alpha\epsilon(x_n) \\
&= \beta\epsilon(x_1) \ldots \beta\epsilon(x_n) \\
&= \beta(\epsilon(x_1) \ldots \epsilon(x_n) \\
&= \beta(x_1 \otimes \cdots \otimes x_n).
\end{aligned}$$

Da $T_R(M)$ von der Menge der $x_1 \otimes \cdots \otimes x_n$ als Modul erzeugt wird, folgt $\alpha = \beta$, so dass die Einzigkeit von α bewiesen ist.

Es sei $n > 0$. Die Abbildung λ_n, die durch

$$\lambda_n(x_1, \ldots, x_n) := \mu(x_1) \ldots \mu(x_n)$$

definiert wird, ist multilinear. Es gibt daher eine R-lineare Abbildung γ_n von $T_R^n(M)$ in A mit

$$\gamma_n(x_1 \otimes \cdots \otimes x_n) = \mu(x_1) \ldots \mu(x_n).$$

Ist e die Eins von A, so setzen wir noch

$$\gamma_0(r) := re$$

für alle $r \in R$. Mittels dieser Abbildungen definieren wir α durch

$$\alpha(f) := \sum_{i:=0}^{\infty} \gamma_i(f_i)$$

für alle $f \in T_R(M)$. Es ist klar, dass α eine lineare Abbildung von $T_R(M)$ in A ist. Nach Konstruktion von α gilt ferner $\alpha\epsilon = \mu$ und $\alpha(1) = e$. Es bleibt zu zeigen, dass α multiplikativ ist. Sind $x_1, \ldots, x_m, y_1, \ldots, y_n \in M$, so folgt (hier erst benutzen wir die Assoziativität der Multiplikation in A)

$$\begin{aligned}\alpha((x_1 \otimes \cdots \otimes x_m)(y_1 \otimes \cdots \otimes y_n)) &= \alpha(x_1 \otimes \cdots \otimes x_m \otimes y_1 \otimes \cdots \otimes y_n) \\ &= \mu(x_1) \ldots \mu(x_m)\mu(y_1) \ldots \mu(y_n) \\ &= \alpha(x_1 \otimes \cdots \otimes x_m)\alpha(y_1 \otimes \cdots \otimes y_n).\end{aligned}$$

Hieraus folgt zusammen mit der Linearität von α die Multiplikativität von α.

Der nächste Satz zeigt, dass die Tensoralgebra eines freien Moduls ein wohlbekanntes Objekt ist. Er wird uns im nächsten Kapitel an einer entscheidenden Stelle weiterhelfen.

1.2. Satz. *Es sei R ein kommutativer Ring mit Eins und F sei ein freier R-Modul. Ferner sei ϵ die vor Satz 1.1 definierte Abbildung von F in $T_R(F)$. Ist B eine Basis von F und bezeichnet $\mathrm{pol}_R(B)$ die freie assoziative Algebra über R in der Menge der Unbestimmten B, so gibt es einen Isomorphismus φ von $\mathrm{pol}_R[B]$ auf $T_R(F)$ mit $\varphi(b) = \epsilon(b)$ für alle $b \in B$.*

Beweis. Die Definition der freien assoziativen Algebra besagt, dass es einen Homomorphismus φ von $\mathrm{pol}_R[B]$ in $T_R(F)$ gibt mit $\varphi(b) = \epsilon(b)$ für alle $b \in B$. Nach 1.1 gibt es einen Homomorphismus ψ von $T_R(F)$ in $\mathrm{pol}_R[B]$ mit $\psi\epsilon(b) = b$ für alle $b \in B$. Es folgt $\psi\varphi(b) = b$ und damit

$$\psi\varphi = 1_{\mathrm{pol}_R[B]}.$$

Andrerseits ist $\varphi\psi\epsilon(b) = \epsilon(b)$ für alle $b \in B$ und damit

$$\varphi\psi = 1_{T_R(F)}.$$

Damit ist alles bewiesen.

Es sei R ein kommutativer Ring mit Eins und M sei ein Modul über R. Ferner sei I das zweiseitige Ideal von $T_R(M)$, welches von allen Elementen der Form $x \otimes x$ mit $x \in M$ erzeugt wird. Wir setzen

$$\textstyle\bigwedge_R(M) := T_R(M)/I$$

und nennen $\bigwedge_R(M)$ die *Graßmannalgebra* von M. Wir setzen ferner

$$\textstyle\bigwedge_R^n(M) := (T_R^n(M) + I)/I.$$

Die Multiplikation in $\bigwedge_R(M)$ bezeichnen wir mit $\wedge$.

Offenbar gilt $I \cap T_R^0(M) = \{0\} = I \cap T_R^1(M)$. Wir dürfen daher $r \in R$ mit $r + I$ und $m \in M$ mit $m + I$ identifizieren.

1.3. Satz. *Es sei R ein kommutativer Ring mit Eins und M sei ein Modul über R. Ferner sei A eine assoziative R-Algebra mit Eins. Ist φ eine R-lineare Abbildung von M in A und gilt $\varphi(x)^2 = 0$ für alle $x \in M$, so gibt es genau einen Homomorphismus ψ von $\bigwedge_R(M)$ in A mit $\psi(x) = \varphi(x)$ für alle $x \in M$.*

Beweis. Dies folgt mit Standardschlüssen aus 1.1.

1.4. Satz. *Es sei R ein kommutativer Ring mit Eins und M und N seien zwei R-Moduln. Ist φ ein Homomorphismus von M in N, so gibt es genau einen Homomorphismus ψ von $\bigwedge_R(M)$ in $\bigwedge_R(N)$ mit $\psi(x) = \varphi(x)$ für alle $x \in M$. Ist φ surjektiv, so ist auch ψ surjektiv. Ferner gilt $\psi(\bigwedge_R^k(M)) \subseteq \bigwedge_R^k(N)$ für alle nicht negativen ganzen Zahlen k.*

Beweis. Existenz und Eindeutigkeit von ψ folgen mit 1.3. Die Aussage, dass $\psi(\bigwedge_R^k(M)) \subseteq \bigwedge_R^k(N)$ ist, gilt für $k = 1$ und folgt dann für beliebiges k durch Induktion. Weil $\bigwedge_R^1(N)$ die Algebra $\bigwedge_R(N)$ erzeugt, ist ψ surjektiv, falls φ surjektiv ist.

Die Abbildung ψ ist nicht notwendig injektiv, wenn φ es ist.

1.5. Satz. *Es sei R ein kommutativer Ring mit Eins und M sei ein R-Modul. Sind $x_1, \ldots, x_n \in M$ und ist σ eine Permutation aus der symmetrischen Gruppe S_n vom Grade n, so gilt*

$$x_{\sigma(1)} \wedge \ldots \wedge x_{\sigma(n)} = \operatorname{sgn}(\sigma) x_1 \wedge \ldots \wedge x_n.$$

Sind i und j zwei verschiedene der Indizes 1, …, n und ist $x_i = x_j$, so ist

$$x_1 \wedge \ldots \wedge x_n = 0.$$

Beweis. Es ist

$$x_1 \wedge x_2 + x_2 \wedge x_1 = (x_1 + x_2) \wedge (x_2 + x_1) - x_1 \wedge x_1 - x_2 \wedge x_2 = 0,$$

so dass die erste Aussage für $n = 2$ richtig ist. Induktion zeigt ihre Gültigkeit für beliebiges n, wenn man nur noch beachtet, dass jede Permutation Produkt von Transpositionen ist.

Nach dem bereits Bewiesenen ist

$$x_1 \wedge \ldots \wedge x_n = \pm x_i \wedge x_j \wedge y$$

mit einem geeigneten y. Wegen $x_i = x_j$ ist aber $x_i \wedge x_j = 0$. Damit ist alles bewiesen.

1.6. Satz. *Es sei R ein kommutativer Ring mit Eins und M sei ein R-Modul. Ist $\{b_1, \ldots, b_n\}$ ein Erzeugendensystem von M, so ist*

$$\bigwedge_R^i(M) = \{0\} \quad \textit{für alle } i > n.$$

Beweis. Es sei $i > n$ und sei $x_1, \ldots, x_i \in M$. Es gibt dann $a_{jk} \in R$ mit

$$x_k = \sum_{j:=1}^{n} b_j a_{jk}.$$

Es folgt

$$x_1 \wedge \ldots \wedge x_i = \sum_{j:=1}^{n} b_j a_{j1} \wedge \ldots \wedge \sum_{j:=1}^{n} b_j a_{ji} = \sum_{\alpha} (b_{\alpha(1)1} \wedge \ldots \wedge b_{\alpha(i)i}) A_\alpha,$$

wobei α die Menge der Abbildungen von $\{1, \ldots, i\}$ in $\{1, \ldots n\}$ durchläuft und $A_\alpha \in R$ gilt. Wegen $n < i$ ist keines der α injektiv, so dass nach 1.5 für alle α die Gleichung

$$b_{\alpha(1)1} \wedge \ldots \wedge b_{\alpha(i)i} = 0$$

gilt. Hieraus folgt die Behauptung.

1.7. Satz. *Es sei R ein kommutativer Ring mit 1 und F sei ein freier Modul über R. Es sei weiter B eine Basis von F, die linear geordnet sei. Ist $J \in \mathrm{Fin}(B)$, sind $b_1, \ldots, b_n$ die Elemente von J und gilt $b_1 < \ldots < b_n$, so setzen wir*

$$b_J := b_1 \wedge \ldots \wedge b_n.$$

Ferner setzen wir $b_\emptyset := 1$. Dann ist $\{b_J \mid J \in \mathrm{Fin}(B)\}$ eine Basis von $\bigwedge_R(F)$.

Beweis. Mit 1.5 folgt, dass $\{b_J \mid J \in \mathrm{Fin}(B)\}$ ein Erzeugendensystem von $\bigwedge_R(F)$ ist. Wir müssen also nur noch zeigen, dass $\{b_J \mid J \in \mathrm{Fin}(B)\}$ auch linear unabhängig ist.

Es sei $\{w_J \mid J \in \mathrm{Fin}(B)\}$ eine mit $\mathrm{Fin}(B)$ indizierte Menge und A sei ein freier R-Modul mit der Basis $\{w_J \mid J \in \mathrm{Fin}(B)\}$. Sind $i, j \in B$, so setzen wir

$$\langle i, j \rangle := \begin{cases} 0, & \text{falls } i = j, \\ 1, & \text{falls } i < j, \\ -1, & \text{falls } i > j. \end{cases}$$

Ferner setzen wir

$$w_I w_J := \Bigl(\prod_{i \in I, j \in J} \langle i, j \rangle \Bigr) w_{I \cup J}.$$

Setzt man die für je zwei Basiselemente definierte Multiplikation linear fort, so wird A eine R-Algebra, wie wir nun sehen werden. Dazu genügt es zu zeigen, dass A eine Eins besitzt und dass

$$(w_I w_J) w_L = w_I (w_J w_L)$$

ist für alle $I, J, L \in \mathrm{Fin}(B)$.

Offenbar ist $w_\emptyset$ das Einselement von A.

Um die Assoziativität zu beweisen, seien I, J, $L \in \mathrm{Fin}(B)$. Ist $I \cap J \neq \emptyset$, so ist $w_I w_J = 0$ und daher $(w_I w_J)w_L = 0$. Andererseits folgt aus $I \cap J \neq \emptyset$, dass auch $I \cap (J \cup L) \neq \emptyset$ ist. Daher ist

$$w_I(w_J w_L) = \pm w_I w_{J \cup L} = 0.$$

In diesem Falle ist also $(w_I w_J)w_L = w_I(w_J w_L)$. Der Fall $I \cap L \neq \emptyset$ erledigt sich analog. Es sei also $I \cap J = \emptyset$ und $J \cap L = \emptyset$. Dann ist

$$\prod_{k \in I \cup J, l \in L} \langle k, l \rangle = \prod_{k \in I, l \in L} \langle k, l \rangle \prod_{k \in J, l \in L} \langle k, l \rangle$$

und daher

$$\begin{aligned}(w_I w_J)w_L &= \prod_{i \in I, j \in J} w_{I \cup J} w_L \\ &= \prod_{i \in I, j \in J} \langle i, j \rangle \prod_{k \in I \cup J, l \in L} \langle k, l \rangle w_{I \cup J \cup L} \\ &= \prod_{i \in I, j \in J} \langle i, j \rangle \prod_{k \in I, l \in L} \langle k, l \rangle \prod_{k \in J, l \in L} \langle k, l \rangle w_{I \cup J \cup L}.\end{aligned}$$

Andererseits ist, da ja $J \cap L = \emptyset$ ist,

$$\begin{aligned}w_I(w_J w_L) &= \prod_{k \in J, l \in L} \langle k, l \rangle w_I w_{J \cup L} \\ &= \prod_{k \in J, l \in L} \langle k, l \rangle \prod_{i \in I, j \in J \cup L} \langle i, j \rangle w_{I \cup J \cup L} \\ &= \prod_{k \in J, l \in L} \langle k, l \rangle \prod_{i \in I, j \in J} \langle i, j \rangle \prod_{k \in J, l \in L} \langle k, l \rangle w_{I \cup J \cup L}.\end{aligned}$$

Also ist $(w_I w_J)w_L = w_I(w_J w_L)$, so dass A in der Tat eine R-Algebra ist.

Es gibt einen Homomorphismus α von F in A mit $\alpha(b) = w_{\{b\}}$. Ist $f = \sum_{b \in B} b f_b$ so folgt

$$\begin{aligned}\alpha(f)^2 &= \sum_{b \in B} \sum_{c \in B} w_{\{b\}} w_{\{c\}} \\ &= \sum_{b \in B} w_{\{b\}}^2 f_b^2 + \sum_{b, c \in B, b < c} (w_{\{b\}} w_{\{c\}} + w_{\{c\}} w_{\{b\}}) f_b f_c = 0.\end{aligned}$$

Es gibt daher einen Homomorphismus β von $\bigwedge_R(F)$ in A mit

$$\alpha(b) = \beta(b)$$

für alle $b \in B$. Hieraus folgt $\beta(b_I) = w_I$ für alle $I \in \mathrm{Fin}(B)$, so dass die b_I in der Tat eine Basis von $\bigwedge_R(F)$ sind. Es folgt weiter, dass β ein Isomorphismus ist. Damit ist alles bewiesen.

Der Beweis des Satzes liefert auch noch die beiden folgenden Korollare.

1.8. Korollar. *Es sei R ein kommutativer Ring mit Eins und F sei ein freier R-Modul. Dann ist*

$$\bigwedge_R(F) = \bigoplus_{k:=0}^{\infty} \bigwedge_R^k(F).$$

1.9. Korollar. *Es sei R ein kommutativer Ring mit Eins und F sei ein freier R-Modul des Ranges n. Dann ist*

$$\mathrm{Rg}_R(\bigwedge_R(F)) = 2^n$$

und

$$\mathrm{Rg}_R(\bigwedge_R^k(F)) = \binom{n}{k}$$

für alle ganzen Zahlen k mit $0 \leq k \leq n$.

Ist B unendlich, so hat $\mathrm{Fin}(B)$ und auch die Menge $\mathrm{Fin}_k(B)$ der k-Teilmengen von B die gleiche Mächtigkeit wie B, so dass $\bigwedge_R(F)$ und $\bigwedge_R^k(F)$ in diesem Falle den gleichen Rang wie F haben.

1.10. Satz. *Es sei K ein kommutativer Körper und V sei ein Vektorraum über K. Sind $v_1, \ldots, v_r \in V$, so sind $v_1, \ldots, v_r$ genau dann linear unabhängig, wenn $v_1 \wedge \ldots \wedge v_r \neq 0$ ist.*

Beweis. Sind $v_1, \ldots, v_r$ linear unabhängig, so sind sie Teil einer Basis von V. Dann gehört aber $v_1 \wedge \ldots \wedge v_r$ nach 1.7 zu einer Basis von $\bigwedge_R(V)$, ist also von 0 verschieden.

Sind $v_1, \ldots, v_r$ linear abhängig, so ist oBdA

$$v_r = \sum_{i:=1}^{r-1} v_i \lambda_i$$

und nach 1.5 folglich

$$v_1 \wedge \ldots \wedge v_r = \sum_{i:=1}^{r-1} ((v_1 \wedge \ldots \wedge v_{r-1}) \wedge v_i)\lambda_i = 0.$$

Damit ist alles bewiesen.

Wir schließen diesen Abschnitt mit einem Satz, den wir nur so formulieren werden, wie wir ihn später benötigen. Zuvor jedoch noch eine Definition. Ist $u \in \bigwedge_K(V)$, so heißt v *zerlegbar*, falls es $v_1, \ldots, v_r \in V$ gibt mit $u = v_1 \wedge \ldots \wedge v_r$.

1.11. Satz. *Es sei V ein Vektorraum über dem kommutativen Körper K. Ist σ ein Endomorphismus von V, so gilt:*

a) *Es gibt genau einen Endomorphismus $\sigma_{\#r}$ von $\bigwedge_K^r(V)$ mit*

$$\sigma_{\#r}(v_1 \wedge \ldots \wedge v_r) = \sigma(v_1) \wedge \ldots \wedge \sigma(v_t)$$

für alle $v_1, \ldots, v_r \in V$. Insbesondere bildet $\sigma_{\#r}$ zerlegbare Vektoren auf zerlegbare Vektoren ab.

b) *Es ist $(\sigma\tau)_{\#r} = \sigma_{\#r}\tau_{\#r}$, falls τ ein weiterer Endomorphismus von V ist.*

c) *Für jeden Automorphismus σ von V ist $\sigma_{\#r}$ ein Automorphismus von $\bigwedge_K^r(V)$.*

d) *Ist $u \in \bigwedge_K^r(V)$ und $v \in \bigwedge_K^s(V)$, so ist*

$$\sigma_{\#r}(u) \wedge \sigma_{\#s}(v) = \sigma_{\#(r+s)}(u \wedge v).$$

Beweis. a) Es seien $v_1, \ldots, v_r \in V$. Nach Satz 1.4 gibt es einen Endomorphismus ρ von $\bigwedge_K(V)$ mit $\sigma(v) = \rho(v)$ für alle $v \in V$. Es sei $\sigma_{\#r}$ die Einschränkung von ρ auf $\bigwedge_K^r(V)$. Dann ist $\sigma_{\#r}$ nach 1.4 ein Endomorphismus von $\bigwedge_K^r(V)$ und es gilt

$$\begin{aligned}\sigma_{\#r}(v_1 \wedge \ldots \wedge v_r) &= \rho(v_1 \wedge \ldots \wedge v_r)\\ &= \rho(v_1) \wedge \ldots \wedge \rho(v_r)\\ &= \sigma(v_1) \wedge \ldots \wedge \sigma(v_r).\end{aligned}$$

b) Es ist

$$\begin{aligned}(\sigma\tau)_{\#r}(v_1 \wedge \ldots \wedge v_r) &= \sigma\tau(v_1) \wedge \ldots \wedge \sigma\tau(v_r)\\ &= \sigma_{\#r}(\tau(v_1) \wedge \ldots \wedge \tau(v_r))\\ &= \sigma_{\#r}\tau_{\#r}(v_1 \wedge \ldots \wedge v_r).\end{aligned}$$

Da $\bigwedge_K^r(V)$ von seinen zerlegbaren Vektoren erzeugt wird, ist somit

$$(\sigma\tau)_{\#r} = \sigma_{\#r}\tau_{\#r}.$$

c) Es ist $(1_V)_{\#r} = 1_{\bigwedge_K^r(V)}$. Ist nun σ ein Automorphismus von V, so folgt mit b)

$$1_{\bigwedge_K^r(V)} = (\sigma\sigma^{-1})_{\#r} = \sigma_{\#r}(\sigma^{-1})_{\#r}$$

und

$$1_{\bigwedge_K^r(V)} = (\sigma^{-1}\sigma)_{\#r} = (\sigma^{-1})_{\#r}\sigma_{\#r}.$$

Also ist auch $\sigma_{\#r}$ ein Automorphismus.

d) Weil u Linearkombination von zerlegbaren Vektoren der Länge r und v Linearkombination von zerlegbaren Vektoren der Länge s ist, ist $u \wedge v$ Linearkombination von zerlegbaren Vektoren der Länge $r+s$, so dass $u \wedge v \in \bigwedge_K^{r+s}(V)$ ist. Hat nun ρ wieder die Bedeutung wie beim Beweise von a), so ist

$$\sigma_{\#r}(u) \wedge \tau_{\#s}(v) = \rho(u) \wedge \rho(v) = \rho(u \wedge v) = \sigma_{\#(r+s)}(u \wedge v).$$

Hieraus folgt die Behauptung unter d).

2. Dualität in der Graßmannalgebra

Es sei K ein kommutativer Körper und V und W seien zwei Vektorräume über K. Die Abbildung f des r-fachen cartesischen Produktes V^r von V mit sich selbst in W heißt *r-fach alternierende Abbildung* von V in W, falls f in jedem Argument linear ist und überdies $f(v_1, \ldots, v_r) = 0$ ist, falls zwei der Argumente gleich sind. Die Menge aller r-fach linearen Abbildungen von V in W bezeichnen wir mit $\mathrm{Alt}_K^r(V, W)$.

2.1. Satz. *Es seien V und W Vektorräume über dem kommutativen Körper K. Ist $f \in \mathrm{Alt}_K^r(V)$ und sind $v_1, \ldots, v_r$ linear abhängige Vektoren aus V, so ist $f(v_1, \ldots, v_r) = 0$.*

Beweis. Es sei oBdA $v_r = \sum_{i:=1}^{r-1} v_i\alpha_i$. Dann ist

$$f(v_1, \ldots, v_r) = \sum_{i:=1}^{r-1} f(v_1, \ldots, v_{r-1}, v_i)\alpha_i = 0.$$

2.2. Korollar. *Es seien V und W Vektorräume über dem kommutativen Körper K. Ist V endlich erzeugt und ist $r > \mathrm{Rg}_K(V)$, so ist $\mathrm{Alt}_K^r(V) = \{0\}$.*

Der Beweis des nächste Satzes ist eine einfache Übungsaufgabe, wenn man nur beachtet, dass die symmetrische Gruppe S_r von ihren Transpositionen erzeugt wird.

2.3. Satz. *Es sei K ein kommutativer Körper und V und W seien Vektorräume über K. Sind $v_1, \ldots, v_r \in V$, ist $\pi \in S_r$ und ist $f \in \mathrm{Alt}_K^r(V, W)$, so ist*

$$f(v_{\pi(1)}, \ldots, v_{\pi(r)}) = \mathrm{sgn}(\pi) f(v_1, \ldots, v_r).$$

Mit $\mathrm{Lin}_K^r(V, W)$ bezeichnen wir die Menge der r-fach linearen Abbildungen von V in W. Ist $f \in \mathrm{Lin}_K^r(V, W)$, so setzen wir

$$fa(v_1, \ldots, v_r) := \sum_{\pi \in S_r} \mathrm{sgn}(\pi) f(v_{\pi(1)}, \ldots, v_{\pi(r)}).$$

Die Abbildung fa heißt die *Antisymmetrisierte* von f. Die Menge der antisymmetrisierten, r-fach linearen Abbildungen von V in W bezeichnen wir mit $\mathrm{Ant}_K^r(V, W)$.

2.4. Satz. *Es seien V und W Vektorräume über dem kommutativen Körper K. Ist r eine natürliche Zahl, so ist*

$$\mathrm{Alt}_K^r(V, W) = \mathrm{Ant}_K^r(V, W).$$

Beweis. Es sei $f \in \mathrm{Lin}_K^r(V, W)$. Ferner seien $v_1, \ldots, v_r \in V$ und es gebe i, j mit $i \neq j$ und $v_i = v_j$. Es sei τ die Transposition, die i mit j vertauscht. Dann ist $S_r = A_r \cup \tau A_r$ und $A_r \cap \tau A_r = \emptyset$. Es folgt

$$fa(v_1, \ldots, v_r) = \sum_{\pi \in A_r} (f(v_{\pi(1)}, \ldots, v_{\pi(r)}) - f(v_{\tau\pi(1)}, \ldots, v_{\tau\pi(r)}).$$

Ist $\pi(k) \neq i, j$, so ist $v_{\tau\pi(k)} = v_{\pi(k)}$. Ist $\pi(k) = i$, so folgt

$$v_{\tau\pi(k)} = v_{\tau(i)} = v_j = v_i = v_{\pi(k)},$$

und ist $\pi(k) = j$, so folgt

$$v_{\tau\pi(k)} = v_{\tau(j)} = v_i = v_j = v_{\pi(k)}.$$

Also ist $v_{\tau\pi(k)} = v_{\pi(k)}$ für alle k und damit

$$fa(v_1, \ldots, v_r) = 0.$$

Dies zeigt, dass $\mathrm{Ant}_K^r(V, W) \subseteq \mathrm{Alt}_K^r(V, W)$ ist.

Es sei $g \in \mathrm{Alt}_K^r(V, W)$. Es sei ferner B eine Basis von V, die linear geordnet sei. Schließlich bezeichne Γ die Menge aller Abbildungen von $\{1, \ldots, r\}$ in B. Die Menge aller r-Tupel $(\gamma_1, \ldots, \gamma_r)$ bildet eine Basis von V^r. Es gibt daher genau ein $f \in \mathrm{Lin}_K^r(V, W)$ mit

$$f(\gamma_1, \ldots, \gamma_r) := \begin{cases} g(\gamma_1, \ldots, \gamma_r), & \text{falls } \gamma_1 < \ldots < \gamma_r, \\ 0, & \text{sonst} \end{cases}$$

für alle $\gamma \in \Gamma$. Es ist

$$fa(\gamma_1, \ldots, \gamma_r) = \sum_{\pi \in S_r} \mathrm{sgn}(\pi) f(\gamma_{\pi(1)}, \ldots, \gamma_{\pi(r)}).$$

Ist γ nicht injektiv, so ist auch $\gamma\pi$ nicht injektiv für alle $\pi \in S_r$. In diesem Falle ist also

$$fa(\gamma_1, \ldots, \gamma_r) = 0 = g(\gamma_1, \ldots, \gamma_r).$$

Ist γ injektiv, so gibt es genau ein $\rho \in S_r$ mit

$$\gamma_{\rho(1)} < \ldots < \gamma_{\rho(r)}.$$

Daher ist

$$\begin{aligned} fa(\gamma_1, \ldots, \gamma_r) &= \mathrm{sgn}(\rho) f(\gamma_{\rho(1)}, \ldots, \gamma_{\rho(r)}) \\ &= \mathrm{sgn}(\rho) g(\gamma_{\rho(1)}, \ldots, \gamma_{\rho(r)}) \\ &= g(\gamma_1, \ldots, \gamma_r). \end{aligned}$$

Somit stimmen fa und g auf einer Basis von V^r überein, so dass $fa = g$ ist.

2.5. Satz. *Es seien V und W Vektorräume über dem kommutativen Körper K. Es sei B eine Basis von V, die linear geordnet sei. Ferner sei Γ die Menge aller streng monoton steigenden Abbildungen von $\{1, \ldots, r\}$ in B. Ist η eine Abbildung von Γ in W, so gibt es genau ein $f \in \mathrm{Alt}_K^r(V, W)$ mit*

$$f(\beta_1, \ldots, \beta_r) = \eta(\beta)$$

für alle $\beta \in \Gamma$.

Beweis. Sind $v_1, \ldots, v_r \in V$, so ist

$$v_j = \sum_{b \in B} b a_{bj}$$

mit einer Matrix a über K. Diese Bezeichnung wollen wir im Folgenden festhalten.

Es sei Δ die Menge aller Abbildungen von $\{1, \ldots, r\}$ in B. Um die Einzigkeitsaussage des Satzes zu beweisen, sei $f \in \mathrm{Alt}_K^r(V, W)$ und $f(b_1, \ldots, b_r) = \eta(\beta)$ für alle $\beta \in \Gamma$. Dann ist

$$\begin{aligned} f(v_1, \ldots, v_r) &= \sum_{\beta \in \Delta} f(\beta_1, \ldots \beta_r) \prod_{i:=1}^{r} a_{\beta_i i} \\ &= \sum_{\beta \in \Gamma} \sum_{\pi \in S_r} f(\beta_{\pi(1)}, \ldots, \beta_{\pi(r)}) \prod_{i:=1}^{r} a_{\beta_i i} \\ &= \sum_{\beta \in \Gamma} \eta(\beta) \sum_{\pi \in S_r} \mathrm{sgn}(\pi) \prod_{i:=1}^{r} a_{\beta_i i}. \end{aligned}$$

Da die rechte Seite nur von β und a abhängt, ist die Einzigkeit von f gezeigt.

Definiert man umgekehrt f durch

$$f(v_1, \ldots, v_r) := \sum_{\beta \in \Gamma} \eta(\beta) \sum_{\pi \in S_r} \mathrm{sgn}(\pi) \prod_{i:=1}^{r} a_{\beta_i i},$$

so verifiziert man leicht, dass f alle gewünschten Eigenschaften hat.

2.6. Satz. *Es seien V und W endlich erzeugte Vektorräume über dem kommutativen Körper K. Setze $n := \mathrm{Rg}_K(V)$ und $m := \mathrm{Rg}_K(W)$. Dann ist*

$$\mathrm{Rg}_K(\mathrm{Alt}_K^r(V, W)) = \binom{n}{r} m.$$

Beweis. Nach 2.2 gilt diese Formel jedenfalls dann, wenn $r > n$ ist, da dann ja $\binom{n}{r} = 0$ ist.

Es sei $r \leq n$. Es sei B eine linear geordnete Basis von V und C sei eine Basis von W. Es sei ferner Γ die Menge der streng monoton wachsenden Abbildungen von $\{1, \ldots, r\}$ in B. Ist $\beta \in \Gamma$ und $c \in C$, so definieren wir die Abbildung $\gamma_{\beta,c}$ von Γ in W durch

$$\gamma_{\beta,c}(\delta) := \begin{cases} c, & \text{falls } \beta = \delta, \\ 0, & \text{falls } \beta \neq \delta. \end{cases}$$

Nach 2.5 gibt es genau ein $f_{\beta,c} \in \mathrm{Alt}_K^r(V, W)$ mit

$$f_{\beta,c}(\delta_1, \ldots, \delta_r) := \begin{cases} c, & \text{falls } \beta = \delta, \\ 0, & \text{falls } \beta \neq \delta. \end{cases}$$

Wir zeigen, dass die $f_{\beta,c}$ eine Basis von $\mathrm{Alt}_K^r(V, W)$ bilden.

Es sei

$$0 = \sum_{\beta \in \Gamma} \sum_{c \in C} k_{\beta,c} f_{\beta,c}.$$

Mit $\gamma \in \Gamma$ folgt

$$0 = \sum_{\beta \in \Gamma} \sum_{c \in C} f_{\beta,c}(\gamma_1, \ldots, \gamma_r) k_{\beta,c} = \sum_{c \in C} \sum_{\beta \in \Gamma} f_{\beta,c}(\gamma_1, \ldots, \gamma_r) k_{\beta,c} = \sum_{c \in C} c k_{\gamma,c}.$$

Daher ist $k_{\gamma,c} = 0$ für alle $\gamma \in \Gamma$ und alle $c \in C$. Somit sind die $f_{\beta,c}$ linear unabhängig.

Es sei $f \in \mathrm{Alt}_K^r(V, W)$ und $\gamma \in \Gamma$. Dann ist

$$f(\gamma_1, \ldots, \gamma_r) = \sum_{c \in C} c k_{c,\gamma}.$$

Setze

$$g := \sum_{\gamma \in \Gamma} \sum_{c \in C} f_{\gamma,c} k_{c,\gamma}.$$

Ist dann $\beta \in \Gamma$, so folgt

$$\begin{aligned} g(\beta_1, \ldots, \beta_r) &= \sum_{\gamma \in \Gamma} \sum_{c \in C} f_{\gamma,c}(\beta_1, \ldots, \beta_r) k_{c,\gamma} = \sum_{c \in C} f_{\beta,c}(\beta_1, \ldots, \beta_r) k_{c,\beta} \\ &= \sum_{c \in C} c k_{c,\beta} = f(\beta_1, \ldots, \beta_r). \end{aligned}$$

Mit 2.5 folgt $f = g$, so dass die $f_{\beta,c}$ den Raum $\mathrm{Alt}_K^r(V, W)$ auch erzeugen.

Weil die $f_{\beta,c}$, wie wir gerade gesehen haben, eine Basis von $\mathrm{Alt}_K^r(V, W)$ bilden, ist

$$\mathrm{Rg}_K(\mathrm{Alt}_K^r(V, W)) = |\Gamma| m = \binom{n}{r} m,$$

q. o. o.

Es sei K ein kommutativer Körper und V und W seien zwei K-Vektorräume. Ist σ eine lineare Abbildung von $T_K^r(V)$ in W, so heißt σ eine *r-fach alternierende* Abbildung, falls $(v_1, \ldots, v_r) \to (v_1 \otimes \ldots \otimes v_r)^\sigma$ eine r-fach alternierende Abbildung ist. Mit $A(T_K^r(V), W)$ bezeichnen wir die Menge der alternierenden Abbildungen von $T_K^r(V)$ in W. Da jede Abbildung aus $\mathrm{Alt}_K^r(V, W)$ sich auf genau eine Weise durch das Tensorprodukt faktorisieren lässt, folgt, dass $A(T_K^r(V), W)$ und $\mathrm{Alt}_K^r(V, W)$ vermöge dieser Faktorisierung kanonisch isomorph sind. Ist $W = K$, so schreiben wir $AT_K^r(V)$ an Stelle des schwerfälligeren Ausdrucks $A(T_K^r(V), K)$. Ist $\mathrm{Rg}_K(V) = n$, so ist $\mathrm{Rg}(AT_K^r(V)) = \binom{n}{k}$.

Mit $NT_K^r(V)$ bezeichnen wir den Teilraum von $T_K^r(V)$, der von allen Vektoren $v_1 \otimes \ldots \otimes v_r$ erzeugt wird, bei denen mindestens zwei der v_i gleich sind.

2.7. Satz. *Es sei K ein kommutativer Körper und V sei ein Vektorraum über K. Ist I das Ideal der Tensoralgebra $T_K(V)$, welches von allen $v \otimes v$ mit $v \in V$ erzeugt wird, so ist*

$$NT_K^r(V) = T_K^r(V) \cap I.$$

Beweis. Mit Satz 1.5 folgt $NT_K^r(V) \subseteq I \cap T_K^r(V)$.

Um die umgekehrte Inklusion zu beweisen, sei $w \in I \cap T_K^r(V)$. Es gibt dann zerlegbare Vektoren $z_1, \ldots, z_t$, in deren Zerlegung Produkte der Form $v \otimes v$ vorkommen, sowie $k_1, \ldots, k_t \in K$ mit

$$w = \sum_{i:=1}^{t} z_i k_i.$$

Ohne die Allgemeinheit einzuschränken, dürfen wir annehmen, dass $z_1, \ldots, z_s \in T_K^r(V)$ und $z_{s+1}, \ldots, z_t \notin T_K^r(V)$ ist. Mit 1.8 folgt dann, setzt man noch

$$C := \bigoplus_{i:=0, i \neq r}^{\infty} T_K^i(V),$$

dass

$$w - \sum_{i:=1}^{s} z_i k_i = \sum_{j:=s+1}^{t} z_j k_j \in T_K^r(V) \cap C = \{0\}$$

ist. Also ist

$$w = \sum_{i:=1}^{s} z_i k_i \in NT_K^r(V).$$

Damit ist der Satz bewiesen.

2.8. Satz. *Es sei V ein Vektorraum über dem kommutativen Körper K. Es gibt genau einen Isomorphismus φ von $T_K^r(V)/NT_K^R(V)$ auf $\bigwedge_K^r(V)$ mit*

$$\varphi(v_1 \otimes \ldots \otimes v_r + NT_K^r(V)) = v_1 \wedge \ldots \wedge v_r.$$

Beweis. Es ist ja $\bigwedge_K^r(V) = (T_K^r(V) + I)/I$, wobei I wieder das Ideal der Tensoralgebra von V ist, welches von den Elementen $v \otimes v$ mit $v \in V$ erzeugt wird. Bezeichnet man mit κ die Einschränkung des kanonischen Epimorphismus von $T_K^r(V) + I$ auf $T_K^r(V)$, so gilt

$$\kappa(v_1 \otimes \ldots \otimes v_r) = v_1 \wedge \ldots \wedge v_r,$$

woraus weiter folgt, dass κ surjektiv ist. Mit 2.7 folgt

$$\mathrm{Kern}(\kappa) = I \cap T_K^r(V) = NT_K^r(V),$$

woraus mittels des ersten Isomorphiesatzes die Behauptung folgt.

Es sei V ein Vektorraum über dem kommutativen Körper K und V^* sei sein Dualraum. Um Klammern zu sparen, schreiben wir wieder fv für das Bild von v unter f, falls $f \in V^*$ und $v \in V$ ist. Sind nun $f_1, \ldots, f_r \in V^*$, so ist

$$(f_1 \otimes \ldots \otimes f_r)(v_1 \otimes \ldots \otimes v_r) = f_1 v_1 \otimes \ldots \otimes f_r v_r = \prod_{i:=1}^{r} f v_i.$$

Dies zeigt, dass $T_K^r(V^*) \subseteq T_K^r(V)^*$ ist. Ist V endlichen Ranges, so ist $T_K^r(V^*) = T_K^r(V)^*$, da beide Vektorräume den Rang $\mathrm{Rg}_K(V)^r$ haben.

2.9. Satz. *Es sei K ein kommutativer Körper. Ist V ein Vektorraum über K, so ist*

$$NT_K^r(V)^\perp = AT_K^r(V).$$

Beweis. Es ist $NT_K^r(V)$ der von allen $v_1 \otimes \ldots \otimes v_r$, bei denen wenigstens zwei der v_i gleich sind, erzeugte Unterraum von $T_K^r(V)$. Nun ist $\sigma \in T_K^r(V)^*$ genau dann alternierend, wenn $NT_K^r(V) \subseteq \mathrm{Kern}(\sigma)$ gilt. Daher ist $AT_K^r(V) = NT_K^r(V)^\perp$, q. e. d.

Es sei $f \in T_K^r(V)$. Wir definieren die Abbildung g von V^r in K durch

$$g(v_1, \ldots, v_r) := f(v_1 \otimes \ldots \otimes v_r).$$

Dann ist g natürlich eine multilineare Abbildung von V in K. Daher gibt es für die Antisymmetrisierte ga von g ein $fa \in T_K^r(V)^*$ mit

$$ga(v_1, \ldots, v_r) = fa(v_1 \otimes \ldots \otimes v_r)$$

für alle $v_1, \ldots, v_r \in V$. Dieses fa nennen wir sinngemäß *Antisymmetrisierte* von f. Es gilt

$$\begin{aligned} fa(v_1 \otimes \ldots \otimes v_r) = ga(v_1, \ldots, v_r) &= \sum_{\pi \in S_r} \mathrm{sgn}(\pi) g(v_{\pi(1)}, \ldots g_{\pi(r)}) \\ &= \sum_{\pi \in S_r} \mathrm{sgn}(\pi) f(v_{\pi(1)} \otimes \ldots \otimes v_{\pi(r)}). \end{aligned}$$

2.10. Satz. *Es sei K ein kommutativer Körper und V sei ein Vektorraum über K. Ferner seien $y_1, \ldots, y_r \in V^*$. Setze*

$$f := y_1 \otimes \ldots \otimes y_r.$$

Dann ist

$$fa = \sum_{\pi \in S_r} \mathrm{sgn}(\pi)(y_{\pi(1)} \otimes \ldots \otimes y_{\pi(r)}).$$

Beweis. Nach der zuvor gemachten Bemerkung folgt mittels $f = y_1 \otimes \ldots \otimes y_r$, dass

$$\begin{aligned} fa(v_1 \otimes \ldots \otimes v_r) &= \sum_{\pi \in S_r} \mathrm{sgn}(\pi) f(v_{\pi(1)} \otimes \ldots \otimes v_{\pi(r)}) \\ &= \sum_{\pi \in S_r} \mathrm{sgn}(\pi) \prod_{i:=1}^{r} y_i v_{\pi(i)} = \sum_{\pi \in S_r} \mathrm{sgn}(\pi) \prod_{i:=1}^{r} y_{\pi(i)} v_i \\ &= \sum_{\pi \in S_r} \mathrm{sgn}(\pi)(y_{\pi(1)} \otimes \ldots \otimes y_{\pi(r)})(v_1 \otimes \ldots \otimes v_r) \end{aligned}$$

ist. Hieraus folgt die Behauptung.

2.11. Satz. *Es sei V ein Vektorraum endlichen Ranges über dem kommutativen Körper K. Es gibt dann genau ein Skalarprodukt f, sodass $(\bigwedge_K^r(V^*), \bigwedge_K^r(V), f)$ ein duales Raumpaar ist und überdies*

$$f(y_1 \wedge \ldots \wedge y_r, x_1 \wedge \ldots \wedge x_r) = \det(y_i x_j \mid i,j := 1, \ldots r)$$

gilt für alle $y_1, \ldots, y_r \in V^*$ und alle $x_1, \ldots, x_r \in V$.

Beweis. Dass es höchstens ein solches Skalarprodukt gibt, folgt daraus, dass $\bigwedge_K^r(V^*)$ von den $y_1 \wedge \ldots \wedge y_r$ und $\bigwedge_K^r(V)$ von den $x_1 \wedge \ldots \wedge x_r$ erzeugt werden.

Mit 2.8 folgt die Existenz eines Epimorphismus ψ von $T_K^r(V^*)$ auf $\bigwedge_K^r(V^*)$ mit

$$\psi(y_1 \otimes \ldots \otimes y_r) = y_1 \wedge \ldots \wedge y_r.$$

Es ist

$$\mathrm{Kern}(\psi) = NT_K^r(V^*).$$

Da die Abbildung $(y_1, \ldots, y_r) \to (y_1 \otimes \ldots \otimes y_r)a$ alternierend ist, ist

$$NT_K^r(V^*) \subseteq \mathrm{Kern}(a).$$

Somit gibt es einen eindeutig bestimmten Homomorphismus η von $\bigwedge_K^r(V^*)$ in $T_K^r(V^*)$ mit $a = \eta\psi$. Insbesondere ist

$$(y_1 \otimes \ldots \otimes y_r)a = \eta(y_1 \wedge \ldots \wedge y_r).$$

Weil die $y_1 \otimes \ldots \otimes y_r$ den Raum $T_K^r(V^*)$ erzeugen, erzeugen die $(y_1 \otimes \ldots \otimes y_r)a$ den Raum $T_K^r(V^*)a$. Folglich ist η ein Epimorphismus von $\bigwedge_K^r(V^*)$ auf $T_K^r(V^*)a$. Mittels 2.4 folgt $AT_K^r(V) = T_K^r(V^*)a$ und daher

$$\mathrm{Rg}(\bigwedge\nolimits_K^r(V^*)) = \binom{n}{r} = \mathrm{Rg}(AT_K^r(V)) = \mathrm{Rg}(T_K^r(V^*)a).$$

Hieraus und aus der Surjektivität von η folgt, dass η auch injektiv ist. Somit ist η also ein Isomorphismus von $\bigwedge_K^r(V^*)$ auf $T_K^r(V^*)a$.

$T_K^r(V^*)a$ ist gerade der zu $NT_K^r(V)$ orthogonale Unterraum von $T_K^r(V^*)$. Ist $y \in T_K^r(V^*)a$ und $x \in T_K^r(V)$, so wird also durch die Vorschrift

$$g(y, x + NT_K^r(V)) := yx$$

ein Skalarprodukt g auf $T_K^r(V^*)a \times T_K^r(V)/NT_K^r(V)$ erklärt. Benutzt man den Isomorphismus φ^{-1} von $\bigwedge_K^r(V)$ auf $T_K^R(V)/NT_K^r(V)$ und den eben bestimmten Isomorphismus η von $\bigwedge_K^r(V^*)$ auf $T_K^r(V^*)a$, so wird

$$(\bigwedge\nolimits_K^r(V^*), \bigwedge\nolimits_K^r(V))$$

zu einem dualen Raumpaar bezüglich f, wenn man f durch die Vorschrift

$$f(y,x) := g(\eta(y), \varphi^{-1}(x))$$

definiert. Ist $x = x_1 \wedge \ldots \wedge x_r$ und $y = y_1 \wedge \ldots \wedge y_r$, so folgt mit Satz 2.10

$$\begin{aligned} f(y,x) &= g((y_1 \otimes \ldots \otimes y_r)a, x_1 \otimes \ldots \otimes x_r + NT_K^r(V)) \\ &= (y_1 \otimes \ldots \otimes y_r)a(x_1 \otimes \ldots \otimes x_r) \\ &= \left(\sum_{\pi \in S_r} \operatorname{sgn}(\pi)(y_{\pi(1)} \otimes \ldots \otimes y_{\pi(r)})\right)(x_1 \otimes \ldots \otimes x_r) \\ &= \sum_{\pi \in S_r} \operatorname{sgn}(\pi) \prod_{i:=1}^{r} y_{\pi(i)} x_i \\ &= \det(y_j x_i \mid j, i := 1, \ldots, r). \end{aligned}$$

Damit ist alles bewiesen.

2.12. Satz. *Es sei K ein kommutativer Körper und V sei ein Vektorraum endlichen Ranges über K. Ferner sei f_r das in 2.11 beschriebene Skalarprodukt auf $\bigwedge_K^r(V^*) \times \bigwedge_K^r(V)$. Ist dann $x = \sum_{i:=0}^n x_i \in \bigwedge_K(V)$ mit $x_i \in \bigwedge_K^i(V)$ und $y = \sum_{i:=0}^n y_i \in \bigwedge_K(V^*)$ mit $y_i \in \bigwedge_K^i(V^*)$ und setzt man*

$$f(y,x) := \sum_{i:=0}^{n} f_i(y_i, x_i),$$

so ist f ein Skalarprodukt auf $\bigwedge_K(V^*) \times \bigwedge_K(V)$.

Ist $b_1, \ldots, b_n$ eine Basis von V und $b_1^*, \ldots, b_n^*$ die zu dieser Basis duale Basis von V^*, so ist

$$\{b_I^* \mid I \in \operatorname{Fin}(\{1, \ldots, n\})\}$$

die zu

$$\{b_I^* \mid I \in \operatorname{Fin}(\{1, \ldots, n\})\}$$

duale Basis von $\bigwedge_K(V^*)$.

Beweis. Es ist banal, dass f ein Skalarprodukt ist.

Es seien I, $J \in \operatorname{Fin}(\{1, \ldots, n\})$. Ist $|I| \neq |J|$, so ist $f(b_I^*, b_J) = 0$. Es sei also $|I| = |J|$. Dann ist

$$f(b_I^*, b_J) = \det(b_i^* b_j \mid i \in I, j \in J).$$

Ist nun $I \neq J$, so gibt es wegen $|I| = |J|$ ein $k \in I - J$. Es folgt $b_k^* b_j = 0$ für alle $j \in J$ und damit $f(b_k^* b_j) = 0$. Ist $I = J$, so ist

$$b_i^* b_j = \begin{cases} 1, & \text{falls } i = j \\ 0, & \text{falls } i \neq j \end{cases}$$

und daher

$$\det(b_i^* b_j \mid i, j \in I) = 1.$$

Damit ist der Satz bewiesen.

Zum Schluss noch eine Übungsaufgabe für den Leser.

2.13. Satz. *Es sei K ein kommutativer Körper und V sei ein Vektorraum endlichen Ranges über K. Ist dann $(\bigwedge_K^r(V^*), \bigwedge_K^r(V), f)$ das in 2.11 beschriebene duale Raumpaar, so gilt $(\sigma^*)_{\#r} = (\sigma_{\#r})^*$ für alle $\sigma \in End_K(V)$.*

3. Innere Produkte

Es sei V ein Vektorraum endlichen Ranges über dem kommutativen Körper K und V^* bezeichne wie üblich seinen Dualraum. Wir betrachten auf $\bigwedge_K(V^*) \times \bigwedge_K(V)$ das in Satz 2.12 definierte Skalarprodukt f. Es sei $y \in \bigwedge_K(V^*)$. Die durch $\varphi_y^*(z) := z \wedge y$ definierte Abbildung φ^* ist eine Endomorphismus von $\bigwedge_K(V^*)$. Die zu φ_y^* duale Abbildung von $\bigwedge_K(V)$ in sich bezeichnen wir mit φ_y. Wir definieren $\llcorner$ durch

$$y \llcorner x := \varphi_y(x)$$

für alle $y \in \bigwedge_K(V^*)$ und alle $x \in \bigwedge_K(V)$. Es gilt dann

$$f(z, y \llcorner x) = f(z, \varphi_y(x)) = f(\varphi_y^*(z), x) = f(z \wedge y, x)$$

für alle y, $z \in \bigwedge_K(V^*)$ und alle $x \in \bigwedge_K(V)$. Wir nennen $y \llcorner x$ *rechtsseitiges inneres Produkt* von y mit x. Entsprechend ist die Abbildung $y \to y \wedge x$ ein Endomorphismus von $\bigwedge_K(V)$. Es gibt also einen Endomorphismus $\lrcorner$ von $\bigwedge_K(V^*)$ in sich mit

$$f(z \lrcorner y, x) = f(z, y \wedge x)$$

für alle $z \in \bigwedge_K(V^*)$ und alle y, $x \in \bigwedge_K(V)$. Wir nennen $z \lrcorner y$ *linksseitiges inneres Produkt* von z mit y.

Wir notieren einige Rechenregeln.

3.1. Satz. *Es sei V ein Vektorraum endlichen Ranges über dem kommutativen Körper K. Dann gilt:*

a) *Es ist $z \llcorner (y+x) = (z \llcorner y)+(z \llcorner x)$ für alle $z \in \bigwedge_K(V^*)$ und alle y, $x \in \bigwedge_K(V)$.*

b) *Es ist $(z+y) \llcorner x = (z \llcorner x)+(y \llcorner x)$ für alle z, $y \in \bigwedge_K(V^*)$ und alle $x \in \bigwedge_K(V)$.*

c) *Es ist $(yk) \llcorner x = y \llcorner (xk) = (y \llcorner x)k$ für alle $y \in \bigwedge_K(V^*)$ und alle $x \in \bigwedge_K(V)$.*

d) *Es ist $(z \wedge y) \llcorner x = z \llcorner (y \llcorner x)$ für alle z, $y \in \bigwedge_K(V^*)$ und alle $x \in \bigwedge_K(V)$.*

Entsprechend gilt:

a′) *Es ist $z \lrcorner (y + x) = (z \lrcorner y) + (z \lrcorner x)$ für alle $z \in \bigwedge_K(V^*)$ und alle y, $x \in \bigwedge_K(V)$.*

b′) *Es ist $(z + y) \lrcorner x = (z \lrcorner x) + (y \lrcorner x)$ für alle z, $y \in \bigwedge_K(V^*)$ und alle $x \in \bigwedge_K(V)$.*

c′) *Es ist $(yk) \lrcorner x = y \lrcorner (xk) = (y \lrcorner x)k$ für alle $y \in \bigwedge_K(V^*)$ und alle $x \in \bigwedge_K(V)$.*

d′) *Es ist $z \lrcorner (y \wedge x) = z \lrcorner (y \lrcorner x)$ für alle z, $y \in \bigwedge_K(V^*)$ und alle $x \in \bigwedge_K(V)$.*

Beweis. a) Es sei $u \in \bigwedge_K(V^*)$. Dann ist

$$\begin{aligned} f(u, z \llcorner (x + y)) &= f(u \wedge z, x + y) \\ &= f(u \wedge z, x) + f(u \wedge z, y) \\ &= f(u, z \llcorner x) + f(u, z \llcorner y) \\ &= f(u, (z \llcorner x) + (z \llcorner y)). \end{aligned}$$

Da u beliebig war, gilt

$$z \llcorner (x + y) = (z \llcorner x) + (z \llcorner y).$$

d′) Es sei $u \in \bigwedge_K(V)$. Dann ist

$$\begin{aligned} f(z \lrcorner (y \wedge x), u) &= f(z, (y \wedge x) \wedge u) \\ &= f(z, y \wedge (x \wedge u)) \\ &= f(z \lrcorner y, x \wedge u) \\ &= f((z \lrcorner y) \lrcorner x, u). \end{aligned}$$

Die restlichen Aussagen beweisen sich analog.

Die Elemente aus $\bigwedge_K^r(V)$ nennen wir auch *r-Vektoren* und die Elemente aus $\bigwedge_K^r(V^*)$ nennen wir *r-Formen*. Ist x ein r-Vektor und y ein s-Vektor, so ist $x \wedge y = 0$, falls $r + s > \mathrm{Rg}_K(V)$ ist. Ist $r + s \leq \mathrm{Rg}_K(V)$, so folgt mit 1.8, dass $x \wedge y$ ein $(r + s)$-Vektor ist. Entsprechendes gilt für r- und s-Formen.

3.2. Satz. *Es sei V ein Vektorraum endlichen Ranges über dem kommutativen Körper K. Ist x ein r-Vektor und y eine s-Form, so gilt:*
a) *Für $r < s$ ist $y \llcorner x = 0$. Ist $r \geq s$, so ist $y \llcorner x$ ein $(r - s)$-Vektor.*
b) *Für $r > s$ ist $y \lrcorner x = 0$. Ist $r \leq s$, so ist $y \lrcorner x$ eine $(s - r)$-Form.*
Ist $r = s$, so ist $y \llcorner x = f(y, x) = y \lrcorner x$. Dabei ist f wieder das oben definierte Skalarprodukt auf $\bigwedge_K(V^*) \times \bigwedge_K(V)$.

Beweis. a) Es sei z eine t-Form. Dann ist

$$f(z, y \llcorner x) = f(z \wedge y, x).$$

Ist $r \neq s + t$, was insbesondere für alle t der Fall ist, falls $r < s$ gilt, so ist $f(z \wedge y, x) = 0$ aufgrund der Definition von f, da $z \wedge y$ ja eine $s + t$-Form ist. Ist $r < s$ so ist also $y \llcorner x = 0$, da ja dann $f(z, y \llcorner x) = 0$ für alle Formen z gilt. Ist $r \geq s$, so ist $f(z, y \llcorner x)$ höchstens dann von Null verschieden, wenn $r = s + t$ ist. Dies impliziert, dass

$$y \llcorner x \in \left(\bigoplus_{t:=0, t \neq r-s}^{n} \bigwedge\nolimits_K^t(V^*) \right)^{\top} = \bigwedge\nolimits_K^{s-r}(V)$$

ist.

b) Es sei u ein t-Vektor. Dann ist

$$f(y \lrcorner x, u) = f(y, x \wedge u).$$

Hieraus erschließt man b) analog zu a).

Ist $r = s$, so ist $y \llcorner x \in \bigwedge_K^0(V) = K$. Also ist, da $f(1, 1) = 1$ ist,

$$y \llcorner x = (y \llcorner x) f(1, 1) = f(y \llcorner x, 1) = f(y, x \wedge 1) = f(y, x)$$

und

$$y \lrcorner x = f(1, 1)(y \lrcorner x) = f(1, y \lrcorner x) = f(1 \wedge y, x) = f(y, x).$$

Damit ist alles bewiesen.

3.3. Satz. *Es sei V ein Vektorraum des Ranges n über dem kommutativen Körper K. Ferner sei z eine n-Form ungleich der Nullform. Definiert man φ durch*

$$\varphi(x) := z \lrcorner x,$$

so ist φ ein Isomorphismus von $\bigwedge_K(V)$ auf $\bigwedge_K(V^*)$. Ist φ_r die Einschränkung von φ auf $\bigwedge_K^r(V)$, so ist φ_r ein Isomorphismus von $\bigwedge_K^r(V)$ auf $\bigwedge_K^{n-r}(V^*)$.

Ist y ein n-Vektor mit $f(z,y) = 1$, und ein solcher existiert stets, so ist

$$\varphi^{-1}(u) = u \llcorner y$$

für alle $u \in \bigwedge_K(V^*)$.

Beweis. Aus 3.1 a′) und c′) folgt, dass φ eine lineare Abbildung von $\bigwedge_K(V)$ in $\bigwedge_K(V^*)$ ist. Es sei $b_1, \ldots, b_n$ eine Basis von V. Dann ist

$$0 \neq b_1 \wedge \ldots \wedge b_n \in \bigwedge_K^n(V).$$

Wegen $\mathrm{Rg}(\bigwedge_K^n(V)) = 1$ ist daher

$$\bigwedge_K^n(V) = (b_1 \wedge \ldots \wedge b_n)K,$$

so dass insbesondere alle n-Vektoren zerlegbar sind. Da dies auch für alle n-Formen gilt, ist

$$z = (b_1^* k) \wedge b_2^* \wedge \ldots \wedge b_n^*,$$

wobei $b_1^*, \ldots, b_n^*$ die zu $b_1, \ldots, b_n$ duale Basis ist. Indem wir b_1 durch $b_1 k^{-1}$ ersetzen, erreichen wir, dass

$$z = b_1^* \wedge b_2^* \wedge \ldots \wedge b_n^*$$

ist. Setze

$$y := b_1 \wedge \ldots \wedge b_n.$$

Dann ist $f(z,y) = 1$.

Es seien L, $J \subseteq \{1, \ldots, n\}$. Dann ist

$$f(\varphi(b_J), b_L) = f(z \lrcorner b_J, b_L) = f(z, b_J \wedge b_L) = \prod_{i \in L, j \in J} \langle j, i \rangle f(b^*_{\{1,\ldots,b_n\}}, b_{J \cup L}).$$

Ist I das Komplement von J in $\{1, \ldots, n\}$, so ist

$$f(b^*_{\{1,\ldots,b_n\}}, b_{J \cup L}) = f(b_I^*, b_L).$$

Beachtet man noch, dass $f(b_I^*, b_L) = 0$ ist für $I \neq L$, so sieht man die Gültigkeit von

$$f(\varphi(b_J), b_L) = \prod_{i \in I, j \in J} \langle j, i \rangle f(b_I^*, b_L).$$

Definiere die Abbildung ξ von $\bigwedge_K(V)$ in $\bigwedge_K(V^*)$ durch

$$\xi(b_J) := \prod_{i \in I, j \in J} \langle j, i \rangle b_I^*,$$

wobei I das Komplement von J in $\{1, \ldots, n\}$ ist. Dann ist

$$f(\xi(b_J), b_L) = \prod_{i \in I, j \in J} \langle j, i \rangle f(b_I^*, b_L).$$

Also ist $f(\varphi(b_J), b_L) = f(\xi(b_J), b_L)$ für alle Teilmengen L und J von $\{1, \ldots, n\}$. Weil die b_L eine Basis von $\bigwedge_K^r(V)$ bilden, folgt $\varphi(b_J) = \xi(b_J)$ und damit schließlich $\varphi = \xi$. Also ist

$$\varphi(b_J) = \prod_{i \in I, j \in J} \langle j, i \rangle b_I^*,$$

wenn nur I das Komplement von J in $\{1, \ldots, n\}$ ist.

Definiere die Abbildung ψ von $\bigwedge_K(V^*)$ in $\bigwedge_K(V)$ durch

$$\psi(u) := u \llcorner y$$

für alle $u \in \bigwedge_K(V^*)$. Vertauscht man in der vorstehenden Argumentation die Rollen von V und V^*, was wegen der Endlichkeit des Ranges möglich ist, so sieht man, dass ψ eine lineare Abbildung ist, für die

$$\psi(b_I^*) = \prod_{i \in I, j \in J} \langle j, i \rangle b_J$$

gilt, falls nur J das Komplement von I in $\{1, \ldots, n\}$ ist. (Wer glaubt, es müsse in der Formel $\langle i, j \rangle$ heißen — ich war mir einen Augenblick auch unsicher —, der rechne!) Aus all dem folgt schließlich

$$\psi\varphi(b_J) = \left(\prod_{i \in I, j \in J} \langle i, j \rangle \right)^2 b_J = b_J$$

und

$$\varphi\psi(b_I^*) = \left(\prod_{i \in I, j \in J} \langle i, j \rangle \right)^2 b_I^* = b_I^*.$$

Somit ist φ bijektiv und $\psi = \varphi^{-1}$.

Weil φ ein Isomorphismus ist, folgt mit 3.2 weiter, dass φ_r ein Isomorphismus von $\bigwedge_K^r(V)$ auf $\bigwedge_K^{n-r}(V^*)$ ist.

3.4. Korollar. *Die Voraussetzungen seien wie bei Satz 3.3. Ferner sei $b_1, \ldots, b_n$ eine Basis von V und b_I mit $I \in \mathrm{Fin}(\{1, \ldots, n\})$ bzw. b_J^* mit $J \in \mathrm{Fin}(\{1, \ldots, n\})$ die von der gegebenen Basis abgeleiteten Basen von $\bigwedge_K(V)$ bzw. $\bigwedge_K(V^*)$. Ist dann I eine Teilmenge von $\{1, \ldots, n\}$ und ist J ihr Komplement, so ist*

$$\varphi(b_J) = \prod_{i \in I, j \in J} \langle j, i \rangle b_I^*$$

und

$$\varphi^{-1}(b_I^*) = \prod_{i \in I, j \in J} \langle j, i \rangle b_J^*.$$

Ist X ein Vektorraum über K und ist $k \in K$, so bezeichnen wir mit μ_k die durch $\mu_k(x) := xk$ definierte lineare Abbildung von X in sich.

3.5. Satz. *Es sei V ein Vektorraum des Ranges n über K. Ist $\sigma \in GL(V)$, so gibt es $k \in K^*$ mit*

$$\varphi\sigma_{\#r}\mu_k = \sigma^{*-1}_{\#(n-r)}\varphi.$$

für alle r mit $0 \leq r \leq n$. Dabei ist φ wieder der in Satz 3.3 definierte Isomorphismus von $\bigwedge_K(V)$ auf $\bigwedge_K(V^*)$.

Beweis. Es sei y der bei der Definition von φ benutzte n-Vektor. Ferner sei $v_1, \ldots, v_n$ eine Basis von V mit $y = v_1 \wedge \ldots \wedge v_n$ und $v_1^*, \ldots, v_n^*$ sei ihre duale Basis. Weil σ ein Automorphismus ist, ist auch $\sigma(v_1), \ldots, \sigma(v_n)$ eine Basis von V. Es folgt

$$0 \neq \sigma(v_1) \wedge \ldots \wedge \sigma(v_n) \in \bigwedge_K^n(V).$$

Es gibt folglich ein $k \in K^*$ mit

$$y = \sigma(v_1 k) \wedge \sigma(v_2) \wedge \ldots \wedge \sigma(v_n).$$

Die zu $v_1 k, v_2, \ldots, v_n$ duale Basis ist $v_1^* k^{-1}, v_2^*, \ldots, v_n^*$. Setze $b_1 := v_1 k$ und $b_i := v_i$ für $i > 1$ sowie $b_1^* := v_1^* k^{-1}$ und $b_i^* := v_i^*$ für $i > 1$. Dann ist also $b_1^*, \ldots, b_n^*$ die zu $b_1, \ldots, b_n$ duale Basis. Ferner ist

$$f(\sigma^{*-1}(b_J^*), \sigma(b_i)) = f(b_j^*, \sigma^{-1}\sigma(b_i)) = f(b_j^*, b_i).$$

Also ist $\sigma^{*-1}(b_1^*), \ldots, \sigma^{*-1}(b_n^*)$ die zu $\sigma(b_1), \ldots, \sigma(b_n)$ duale Basis. Ist nun i eine streng monoton steigende Abbildung von $\{1, \ldots, r\}$ in $\{1, \ldots, n\}$ und j eine streng monoton steigende Abbildung von $\{1, \ldots, n-r\}$ auf $\{1, \ldots, n\} - \{i_{\{1,\ldots,r\}}\}$,so folgt mit 3.4

$$\begin{aligned}
\varphi\sigma_{\#r}(b_{i_1} \wedge \ldots \wedge b_{i_r}) &= \varphi(\sigma(b_{i_1}) \wedge \ldots \wedge \sigma(b_{i_r})) \\
&= \prod_{l:=1}^{n-r} \prod_{m:=1}^{r} \langle j_l, i_m \rangle (\sigma^{*-1}(b_{j_1}^*) \wedge \ldots \wedge \sigma^{*-1}(b_{j_{n-r}}^*)) \\
&= \prod_{l:=1}^{n-r} \prod_{m:=1}^{r} \langle j_l, i_m \rangle \sigma^{*-1}_{\#(n-r)}(b_{j_1}^* \wedge \ldots \wedge b_{j_{n-r}}^*).
\end{aligned}$$

Wegen der Monotonie von i und j ist entweder $i_1 = 1$ oder $j_1 = 1$. Diese beiden Fälle sind nun zu unterschieden.

Es sei $i_1 = 1$. Dann ist also

$$\begin{aligned}
\varphi\sigma_{\#r}\mu_k(v_1 \wedge v_{i_2} \wedge \ldots \wedge v_{i_r}) &= \prod_{l:=1}^{n-r} \prod_{m:=1}^{r} \langle j_l, i_m \rangle \sigma^{*-1}_{\#(n-r)}(v_{j_1}^* \wedge \ldots \wedge v_{j_{n-r}}^*) \\
&= \sigma^{*-1}_{\#(n-r)}(v_1 \wedge v_{i_2} \wedge \ldots \wedge v_{i_r}).
\end{aligned}$$

Ist $j_1 = 1$, so ist

$$\begin{aligned}\varphi\sigma_{\#r}(v_{i_1} \wedge \ldots \wedge v_{i_r}) &= \prod_{l:=1}^{n-r} \prod_{m:=1}^{r} \langle j_l, i_m \rangle \sigma^{*-1}_{\#(n-r)} \mu_k^{-1} (v_1^* \wedge v_{j_2}^* \wedge \ldots \wedge v_{j_{n-r}}) \\ &= \sigma^{*-1}_{\#(n-r)} \mu_k^{-1} \varphi(v_{i_1} \wedge \ldots \wedge v_{i_r})\end{aligned}$$

Da die $v_{i_1} \wedge \ldots \wedge v_{i_r}$ eine Basis von $\bigwedge_K(V)$ bilden und da μ_k mit φ vertauschbar ist, gilt also

$$\varphi\sigma_{\#r}\mu_k = \sigma^{*-1}_{\#(n-r)}\varphi.$$

4. Zerlegbare Vektoren

Zerlegbare Vektoren sind für die Geometrie von besonderer Bedeutung, da sich mit ihrer Hilfe die Unterräume von Vektorräumen darstellen lassen. Daher werden wir nun einige Aussagen über sie beweisen. Einige der Sätze gelten auch in allgemeineren Situationen. Wir beschränken uns aber im Folgenden auf Vektorräume, da man die Beweise der fraglichen Sätze abkürzen kann, indem man Eigenschaften benutzt, die nur Vektorräume besitzen.

4.1. Satz. *Es sei K ein kommutativer Körper und V sei ein Vektorraum über K. Ist $0 \neq z \in \bigwedge_K^r(V)$, so setzen wir*

$$V_z := \{x \mid x \in V, z \wedge x = 0\}.$$

Dann ist $V_z \in \mathrm{L}(V)$. Sind $x_1, \ldots, x_s$ linear unabhängige Vektoren aus V_z, so ist $s \leq r$ und es gibt ein $w \in \bigwedge_K^{r-s}(V)$ mit

$$z = w \wedge x_1 \wedge \ldots \wedge x_s.$$

Insbesondere ist $\mathrm{Rg}_K(V_z) \leq r$.

Beweis. Es ist klar, dass V_z ein Unterraum von V ist. Es gibt eine Basis B von V mit $x_1, \ldots, x_s \in B$. Es gibt ferner eine lineare Ordnung von B mit

$$x_1 < x_2 < \ldots < x_s.$$

Nach 1.7 ist

$$z = \sum_{I \in \mathrm{Fin}_r(B)} b_I k_I.$$

Wegen $x_i \in V_z$ ist

$$0 = z \wedge x_i = \sum_{I \in \mathrm{Fin}_r(B)} (b_I \wedge x_i) k_I.$$

Mit 1.7 folgt hieraus

$$(b_I \wedge x_i) k_I = 0$$

für alle $I \in \mathrm{Fin}_r(B)$. Ist $x_i \notin I$, so ist $b_I \wedge x_i \neq 0$ und daher $K_I = 0$. Ist $k_I \neq 0$, so ist also $x_i \in I$ für $i := 1, \ldots, r$. Weil z nicht Null ist, gibt es ein I mit

$|I| = r$ und $k_I \neq 0$. Für dieses I gilt dann also $x_i \in I$ für $i := 1, \ldots, s$. Also ist $s \leq |I| = r$.

Ist $k_I \neq 0$, so ist $x_1, \ldots, x_s \in I$, wie wir gerade gesehen haben. Es gibt dann also ein $w_I \in \bigwedge_K^{r-s}(V)$ mit

$$b_I = w_I \wedge x_1 \wedge \ldots \wedge x_s.$$

Ist $K_I = 0$, so ersetzen wir b_I und w_I jeweils durch 0 und nennen diese Elemente wiederum b_I und w_I. Dann ist also in jedem Falle

$$b_I = w_I \wedge x_1 \wedge \ldots \wedge x_s.$$

Hiermit folgt

$$\begin{aligned} z = \sum_{I \in \mathrm{Fin}_r(B)} b_I k_I &= \sum_{I \in \mathrm{Fin}_r(B)} (w_I \wedge x_1 \wedge \ldots \wedge x_s) k_I \\ &= \Big(\sum_{I \in \mathrm{Fin}_r(B)} w_I k_I \Big) \wedge x_1 \wedge \ldots \wedge x_s. \end{aligned}$$

Damit ist alles bewiesen.

Ist $z \in \bigwedge_K^r(V)$, so heißt z genau dann *zerlegbar*, wenn es $x_1, \ldots, x_r \in V$ gibt mit

$$z = x_1 \wedge \ldots \wedge x_r.$$

4.2. Korollar. *Es sei K ein kommutativer Körper und V ein K-Vektorraum. Ist $0 \neq z \in \bigwedge_K^r(V)$, so ist z genau dann zerlegbar, wenn $\mathrm{Rg}_K(V_z) = r$ ist. Ist $z = x_1 \wedge \ldots \wedge x_r$, so ist*

$$V_z = \sum_{i:=1}^r x_i K.$$

Beweis. Es sei $z = x_1 \wedge \ldots \wedge x_r$ mit $x_i \in V$. Dann ist $z \wedge x_i = 0$ und somit $x_i \in V_z$ für alle i. Weil $x_1, \ldots, x_r$ nach 1.10 linear unabhängig sind, ist $r \leq \mathrm{Rg}_K(V_z)$. Nach 1.10 ist andererseits $\mathrm{Rg}_K(V_z) \leq r$, so dass $\mathrm{Rg}_K(V_z) = r$ ist. Hieraus folgt wiederum $V_z = \sum_{i:=1}^r x_i K$.

Ist umgekehrt $\mathrm{Rg}_K(V_z) = r$ und ist $x_1, \ldots, x_r$ eine Basis von V_z, so gibt es nach 4.1 ein $k \in \bigwedge_K^{r-r}(V) = K$ mit $z = k \wedge x_1 \wedge \ldots \wedge x_r = (kx_1) \wedge \ldots \wedge x_r$. Damit ist das Korollar bewiesen.

4.3. Satz. *Es sei K ein kommutativer Körper und V sei ein K-Vektorraum. Sind $x_1, \ldots, x_r$ und $y_1, \ldots, y_r$ je r linear unabhängige Vektoren aus V, so ist genau dann*

$$\sum_{i:=1}^r x_i K = \sum_{i:=1}^r y_i K,$$

wenn $(x_1 \wedge \ldots \wedge x_r)K = (y_1 \wedge \ldots \wedge y_r)K$ ist.

Beweis. Es sei $(x_1 \wedge \ldots \wedge x_r)K = (y_1 \wedge \ldots \wedge y_r)K$. Es gibt dann ein $k \in K$ mit

$$y_1 \wedge \ldots \wedge y_r = (x_1 \wedge \ldots \wedge x_r)k.$$

Es folgt

$$y_1 \wedge \ldots \wedge y_r \wedge x_i = 0$$

und damit, wenn man noch 4.2 berücksichtigt,

$$x_i \in V_{y_1 \wedge \ldots \wedge y_r} = \sum_{j:=1}^{r} y_j K$$

für alle i. Also gilt

$$\sum_{i:=1}^{r} x_i K \leq \sum_{i:=1}^{r} y_i K.$$

Aus Symmetriegründen gilt auch die umgekehrte Inklusion, so dass in der Tat

$$\sum_{i:=1}^{r} x_i K = \sum_{i:=1}^{r} y_i K$$

gilt.

Es sei nun $\sum_{i:=1}^{r} x_i K = \sum_{i:=1}^{r} y_i K$. Nach 4.2 ist

$$\sum_{i:=1}^{r} y_i K = V_{y_1 \wedge \ldots \wedge y_r}.$$

Nach 1.10 gibt es daher ein $k \in \bigwedge_K^{r-r}(V)$ mit

$$y_1 \wedge \ldots \wedge y_r = k \wedge x_1 \wedge \ldots \wedge x_r = (x_1 \wedge \ldots \wedge x_r)k.$$

Es folgt

$$(y_1 \wedge \ldots \wedge y_r)K \leq (x_1 \wedge \ldots \wedge x_r)K.$$

Aus Symmetriegründen ist dann

$$(y_1 \wedge \ldots \wedge y_r)K = (x_1 \wedge \ldots \wedge x_r)K.$$

Damit ist alles bewiesen.

4.4. Satz. *Es sei K ein kommutativer Körper und V sei ein Vektorraum über K. Ferner sei $0 \neq x \in \bigwedge_K^r(V)$ und $0 \neq y \in \bigwedge_K^s(V)$ und x und y seien beide zerlegbar. Genau dann ist $V_x \leq V_y$, wenn $r \leq s$ ist und es ein $z \in \bigwedge_K^{s-r}(V)$ gibt mit $y = z \wedge x$.*

Beweis. Es sei $x = x_1 \wedge \ldots \wedge x_r$. Dann ist $V_x = \sum_{i:=1}^{r} x_i K$. Überdies sind $x_1, \ldots, x_r$ nach 1.10 linear unabhängig.

Es sei nun $V_x \leq V_y$. Dann sind also $x_1, \ldots, x_r$ linear unabhängige Vektoren aus V_y. Nach 3.10 ist daher $r \leq s$ und es gibt ein $z \in \bigwedge_K^{s-r}(V)$ mit $y = z \wedge x$.

Es sei umgekehrt $y = w \wedge x$ mit einem $w \in \bigwedge_K^{s-r}(V)$. Dann ist

$$y \wedge x_i = w \wedge x \wedge x_i = 0$$

und folglich

$$V_x = \sum_{i:=1}^{r} x_i K \leq V_y.$$

Damit ist 4.4 bewiesen.

4.5. Satz. *Es sei K ein kommutativer Körper und V sei ein Vektorraum über K. Ferner seien x und y zerlegbare Vektoren ungleich Null aus $\bigwedge_K(V)$. Genau dann ist $V_x \cap V_y \neq \{0\}$, wenn $x \wedge y = 0$ ist.*

Beweis. Es sei $V_x \cap V_y \neq \{0\}$. Ist $u_1, \ldots, u_r$ eine Basis von $V_x \cap V_y$ und setzt man $z := u_1 \wedge \ldots \wedge u_r$, so folgt mit 4.2, dass $V_x \cap V_y = V_z$ ist. Nach 4.1 ist $y = z \wedge u$ und $x = w \wedge z$ mit gewissen u und w. Es folgt

$$x \wedge y = w \wedge z \wedge z \wedge u = 0,$$

da wegen der Zerlegbarkeit von z ja $z \wedge z = 0$ ist.

Es sei $V_x \cap V_y = \{0\}$ und $x = x_1 \wedge \ldots \wedge x_r$ sowie $y = y_1 \wedge \ldots \wedge y_s$. Dann ist $x_1, \ldots, x_r$ eine Basis von V_x und $y_1, \ldots, y_s$ eine Basis von V_y. Wegen $V_x \cap V_y = \{0\}$ ist $x_1, \ldots, x_r, y_1, \ldots, y_s$ eine Basis von $V_x + V_y$. Also ist

$$x \wedge y = x_1 \wedge \ldots \wedge x_r \wedge y_1 \wedge \ldots \wedge y_s \neq 0.$$

Damit ist alles bewiesen.

Es sei z eine n-Form ungleich der Nullform. Wir definieren wie in Satz 3.3 den Isomorphismus φ von $\bigwedge_K(V)$ auf $\bigwedge_K(V^*)$ durch $\varphi(x) := z \lrcorner x$.

4.6. Satz. *Es sei V ein Vektorraum endlichen Ranges über dem kommutativen Körper K. Ist $x \in \bigwedge_K(V)$, so ist x genau dann zerlegbar, wenn $\varphi(x)$ zerlegbar ist.*

Beweis. Ist $x = 0$, so ist $\varphi(x) = 0$ und x und $\varphi(x)$ sind zerlegbar. Es sei also $x \neq 0$. Ferner sei $x = x_1 \wedge \ldots \wedge x_r$ mit $x_i \in V$ für alle i. Nach 1.10 sind die x_i linear unabhängig, da ja $x \neq 0$ ist. Sie können also zu einer Basis $x_1, \ldots, x_r, \ldots, x_n$ von V ergänzt werden. Es sei $x_1^*, \ldots, x_n^*$ die zu $x_1, \ldots, x_n$ duale Basis. Ist $r = n$, so ist $\varphi(x) \in \bigwedge_K^0(V)$, so dass auch $\varphi(x)$ zerlegbar ist. Es sei also $r < n$. Indem wir x_n gegebenenfalls durch einen Skalar abändern, können wir erreichen, dass

$$z = x_1^* \wedge \ldots \wedge x_n^*$$

ist, wobei z die zur Konstruktion von φ benutzte n-Form ist. Nach 3.4 ist daher

$$\varphi(x) = (-1)^{(n-r)r} x_{r+1}^* \wedge \ldots \wedge x_n^*,$$

so dass $\varphi(x)$ zerlegbar ist.

Die Umkehrung ist ebenso trivial zu beweisen.

4.7. Korollar. *Jeder $(n-1)$-Vektor ist zerlegbar.*

Beweis. Dies folgt aus 4.6 und 3.3, wenn man nur noch bemerkt, dass 1-Formen trivialerweise zerlegbar sind.

Sind x, $y \in \bigwedge_K(V)$, so setzen wir

$$x \vee y := \varphi^{-1}(\varphi(x) \wedge \varphi(y)).$$

Mit dieser Bezeichnung gilt:

4.8. Satz. *Es sei V ein Vektorraum des Ranges n über dem kommutativen Körper K. Ferner sei $r < n$. Ist $u \in \bigwedge_K^r(V)$, so ist u genau dann zerlegbar, wenn für alle zerlegbaren $(n-r-1)$-Vektoren x gilt, dass $u \vee (u \wedge x) = 0$ ist.*

Beweis. Es sei u zerlegbar. Ferner sei x ein zerlegbarer $(n-r-1)$-Vektor. Ist $u \wedge x = 0$, so ist nichts zu beweisen. Es sei also $u \wedge x \neq 0$ und $u = z_1 \wedge \ldots \wedge u_r$ und $x = u_{r+1} \wedge \ldots \wedge u_{n-1}$. Nach 1.10 sind die Vektoren $u_1, \ldots, u_{n-1}$ linear unabhängig. Es gibt also einen Vektor u_n, so dass $u_1, \ldots, u_n$ eine Basis von V ist. Es sei $u_1^*, \ldots, u_n^*$ die zu $u_1, \ldots, u_n$ duale Basis. Indem wir gegebenenfalls u_n um einen Skalarfaktor abändern, dürfen wir annehmen, dass

$$y = u_1 \wedge \ldots \wedge u_n$$

und

$$z = u_1^* \wedge \ldots \wedge u_n^*$$

ist, wobei y der n-Vektor und z die n-Form aus Satz 3.3 sind. Nach 3.4 ist

$$\varphi(u \wedge x) = \varphi(u_1 \wedge \ldots \wedge u_{n-1}) = (-1)^{n-1} u_n^*$$

und

$$\varphi(u) = \varphi(u_1 \wedge \ldots \wedge u_r) = (-1)^{n(n-r)}(u_{r+1}^* \wedge \ldots \wedge u_n^*).$$

Somit ist $\varphi(u) \wedge \varphi(u \wedge x) = 0$ und daher auch $u \vee (u \wedge x) = 0$.

Es sei nun umgekehrt $u \vee (u \wedge x) = 0$ für alle $(n-r-1)$-Vektoren x. Ferner sei $x_1, \ldots, x_n$ eine Basis von V und x_I mit $I \in \mathrm{Fin}(\{1, \ldots n\})$ sei die dieser Basis entsprechende Basis von $\bigwedge_K(V)$. Dann ist

$$u = \sum_{I \in \mathrm{Fin}_r(V)} x_I k_I$$

mit $k_I \in K$ für alle I. Ist $u = 0$, so ist u zerlegbar. Es sei also $u \neq 0$. Es gibt dann ein $L \in \mathrm{Fin}_r(\{1, \ldots, n\})$ mit $k_L \neq 0$. Die Menge

$$\{1, \ldots, n\} - L$$

enthält $n-r$ Elemente und daher auch $n-r$ Teilmengen der Länge der Länge $n-r-1$. Diese seien $J_1, \ldots, J_{n-r}$. Dann ist

$$u \wedge x_{J_i} = \sum_{|I|=r} (x_I \wedge x_{J_i}) k_I.$$

Nun ist $x_I \wedge x_{J_i} = 0$, falls $I \cap J_i \neq \emptyset$. Es sei $I \cap J_i = \emptyset$. Ferner sei

$$\{1, \ldots, n\} = L \cup J_i \cup \{a_i\}.$$

Ist nun $I \neq L$, so folgt aus

$$I = I \cap (L \cup J_i \cup \{a_i\}) = (I \cap L) \cup (I \cap J_i) \cup (L \cap \{a_i\}) = (I \cap L) \cup (L \cap \{a_i\}),$$

dass $a_i \in L$ und $|I \cap L| = r - 1$ ist. Also ist $I = A \cup \{a_i\}$ mit einer $(r-1)$-Teilmenge A von L. Hieraus folgt, dass

$$u \wedge x_{J_i} = (x_L \cap x_{J_i})k_L + \sum_{A \in \mathrm{Fin}_r(L)} (x_{A \cup \{a_i\}} \wedge x_{J_i}) k_{A \cup \{a_i\}}$$

ist. Es sei $0 = \sum_{i:=1}^{n-r} (u \wedge x_{J_i}) l_i$. Dann ist

$$\begin{aligned} 0 &= \sum_{i:=1}^{n-r} (x_L \wedge x_{J_i}) k_L l_i + \sum_{i:=1}^{n-r} \sum_{A \in \mathrm{Fin}_r(L)} (x_{A \cup \{a_i\}} \wedge x_{J_i}) k_{A \cup \{a_i\}} l_i \\ &= \sum_{i:=1}^{n-r} \pm (x_{L \cup J_i}) k_L l_i + \sum_B x_B \kappa_B. \end{aligned}$$

Dabei sind die B von der Form $A \cup \{a_i\} \cup J_i$. Nun folgt aus $L \cap J_i = \emptyset$ für alle i, dass $L \cup J_i = L \cup J_j$ impliziert, dass $i = j$ ist. Ferner ist $L \cup J_i \neq B = A \cup \{a_j\} \cup J_j$, da sonst $L \cap (\{a_j\} \cup J_j) \neq \emptyset$ wäre. Daher sind die Vektoren $x_{L \cup J_i}$ und x_M linear unabhängig. Hieraus folgt, dass $\pm k_L l_i = 0$ ist für $i := 1, \ldots, n - r$. Wegen $k_L \neq 0$ sind daher alle $l_i = 0$. Dies besagt, dass die $n - r$ Vektoren $u \wedge x_{J_i}$ linear unabhängig sind. Weil $u \wedge x_{J_i}$ ein $(n-1)$-Vektor ist, ist $\varphi(u \wedge x_{J_i})$ eine 1-Form, dh. es ist $\varphi(u \wedge x_{J_i}) \in V^*$. Nun ist $u \vee (u \wedge x_{J_i}) = 0$ für alle i. Daher ist auch $\varphi(u) \wedge \varphi(u \wedge x_{J_i}) = 0$ für alle i und damit

$$\varphi(u \wedge x_{J_i}) \in V^*_{\varphi(u)}.$$

Weil φ ein Isomorphismus ist, folgt

$$\mathrm{Rg}_K(V^*_{\varphi(u)} \geq n - r.$$

Weil u ein r-Vektor ist, ist $\varphi(u)$ nach 3.3 eine $(n-r)$-Form. Nach 4.1 ist andererseits

$$\mathrm{Rg}_K(V^*_{\varphi(u)}) \leq n - r.$$

Daher ist $\mathrm{Rg}_K(V^*_{\varphi(u)}) = n - r$, so dass $\varphi(u)$ nach 4.2 eine zerlegbare $(n-r)$-Form ist. Mit 4.6 folgt, dass auch u zerlegbar ist. Damit ist der Satz bewiesen.

5. Doppelverhältnisse

Doppelverhältnisse spielten in der projektiven Geometrie lange Zeit eine herausragende Rolle. Wir benötigen sie nur, um projektive Kollineationen papposscher Räume zu kennzeichnen, da uns diese Kennzeichnung im nächsten Abschnitt

bequem sein wird. Wir werden uns hier daher kurz fassen. Wer mehr über Doppelverhältnisse wissen möchte, der sei an Baer 1952, S. 71–94 verwiesen.

Es sei V ein Vektorraum des Ranges 2 über dem kommutativen Körper K. Ferner seien P, Q, R und S vier verschiedene Punkte von $\mathrm{L}(V)$. Es gibt dann Vektoren $p \in P$ und $q \in Q$ mit $P = pK$, $Q = qK$ und $R = (p + q)K$. Es gibt ferner ein $d \in K$ mit $S = (p+qd)K$. Wir nennen d *Doppelverhältnis* der Punkte P, Q, R, S. Es gilt nun der folgende Satz.

5.1. Satz. *Es sei V ein Vektorraum des Ranges 2 über dem kommutativen Körper K. Sind P, Q, R und S vier verschiedene Punkte von $\mathrm{L}(V)$, so haben P, Q, R, S genau ein Doppelverhältnis. Dieses bezeichnen wir mit $DV(P, Q; R, S)$.*

Beweis. Die Existenzaussage wurde schon bewiesen. Um die Eindeutigkeit zu beweisen, seien d und d' zwei Doppelverhältnisse der Punkte P, Q, R und S. Es gibt dann von Null verschiedene Vektoren p, $p' \in P$ und q, $q' \in Q$ mit

$$R = (p + q)K = (p' + q')K$$

und

$$S = (p + qd)K = (p' + q'd')K.$$

Es gibt also a, $b \in K$ mit

$$p + q = (p' + q')a$$

und

$$p + qd = (p' + q'd')b.$$

Ferner gibt es u, $v \in K$ mit $p' = pu$ und $q' = qv$. Also ist

$$p + q = pua + qva$$

und

$$p + qd = pub + qvd'b.$$

Es folgt

$$1 = va = ua = ub$$

und damit $u = v = a^{-1}$ und $b = a$. Daher ist $d = a^{-1}d'a = d'$.

Ist K nicht kommutativ, so zeigt eine Analyse des gerade geführten Beweises, dass die Doppelverhältnisse von vier Punkten, die genauso definiert werden, wie hier geschehen, eine Konjugiertenklasse von Elementen aus K^* ausmachen. Diese Analyse ist bei Baer *loc. cit.* durchgeführt.

Sind X und Y zwei Unterräume des Ranges $r - 1$ und $r + 1$ eines Vektorraumes, so hat der Faktorraum Y/X den Rang 2, daher ist auch das Doppelverhältnis von vier Unterräumen des Ranges r definiert, solange diese Unterräume X enthalten und in Y enthalten sind. Diese Bemerkung machen wir uns beim nächsten Satz zunutze.

5.2. Satz. *Es sei V ein Vektorraum endlichen Ranges über dem kommutativen Körper K. Ferner sei $\mathrm{Rg}_K(V) \geq 3$ und κ sei eine Kollineation oder Korrelation von $\mathrm{L}(V)$. Dann sind äquivalent:*

a) *κ ist projektiv.*
b) *Sind X und Y Unterräume von V des Ranges $r-1$ und $r+1$ und sind P, Q, R, S verschiedene Unterräume des Ranges r, die allesamt zwischen X und Y liegen, so ist*

$$DV(P,Q;R,S) = DV(\kappa(P),\kappa(Q);\kappa(R),\kappa(S)).$$

c) *Es gibt zwei Unterräume X und Y von V des Ranges $r-1$ und des Ranges $r+1$, so dass*

$$DV(P,Q;R,S) = DV(\kappa(P),\kappa(Q);\kappa(R),\kappa(S))$$

gilt für alle Quadrupel verschiedener Unterräume P, Q, R, S des Ranges r, die zwischen X und Y liegen.

Beweis. Es seien X und Y zwei Unterräume des Ranges $r-1$ bzw. $r+1$ von V und P, Q, R und S seien vier verschiedene Unterräume des Ranges r, die alle zwischen X und Y liegen. Es gibt dann Vektoren p und q mit $P = X + pK$, $Q = X + qK$, $R = X + (p+q)K$ und $S = X + (p+qd)K$. Dann ist d das Doppelverhältnis der Punkte P, Q, R und S.

Es sei zunächst κ eine Kollineation von $\mathrm{L}(V)$. Nach dem zweiten Struktursatz gibt es dann eine semilineare Abbildung σ von V, die κ induziert. Es sei α der Begleitautomorphismus von σ. Es folgt

$$\begin{aligned}
\kappa(P) &= \kappa(X) + \sigma(p)K \\
\kappa(Q) &= \kappa(X) + \sigma(q)K \\
\kappa(R) &= \kappa(X) + (\sigma(p) + \sigma(q))K \\
\kappa(S) &= \kappa(X) + (\sigma(p) + \sigma(q)d^\alpha)K
\end{aligned}$$

und damit

$$DV(\kappa(P),\kappa(Q);\kappa(R),\kappa(S)) = d^\alpha.$$

Es sei κ eine Korrelation und f sei eine κ darstellende α-Semibilinearform. Es gibt dann Vektoren p' und q' und ein $d' \in K$ mit

$$\begin{aligned}
P^\kappa &= X^\kappa \cap (pK)^\kappa = Y^\kappa + p'K \\
Q^\kappa &= X^\kappa \cap (qK)^\kappa = Y^\kappa + q'K \\
R^\kappa &= X^\kappa \cap ((p+q)K)^\kappa = Y^\kappa + (p'+q')K \\
S^\kappa &= x^\kappa \cap ((p+qd)K)^\kappa = Y^\kappa + (p'+q'd')K.
\end{aligned}$$

Es folgt $f(p,p') = 0 = f(q,q')$ und $f(p,q') \neq 0 \neq f(q,p')$. Weiter folgt

$$0 = f(p+q, p'+q') = f(p,q') + f(q,p')$$

und damit $f(p,q') = -f(q,p')$. Hieraus folgt schließlich

$$0 = f(p+qd, p'+q'd') = f(p,q')(d' - d^\alpha),$$

so dass wegen $f(p,q') \neq 0$ auch hier

$$DV(\kappa(P), \kappa(Q); \kappa(R); \kappa(S)) = d^\alpha$$

ist.

a) impliziert b): Ist κ projektiv, so ist in den vorstehenden Ausführungen $\alpha = 1$, so dass b) in der Tat eine Folge von a) ist.

b) impliziert c): Banal.

c) impliziert a): κ werde durch die semilineare Abbildung σ mit dem Begleitautomorphismus α induziert bzw. durch eine α-Form dargestellt. Ferner seien P und Q zwei verschiedene Unterräume des Ranges r, die zwischen X und Y liegen. Es gibt dann Vektoren p und q mit $P = X + pK$ und $Q = X + qK$. Setze $R := X + (p+q)K$. Es sei $d \in K$ und $d \neq 0, 1$. Setze $S := X + (p+qd)K$. Dann sind P, Q, R und S vier verschiedene Unterräume des Range r, die alle zwischen X und Y liegen. Es folgt

$$d = DV(P, Q, R, S) = DV(\kappa(P), \kappa(Q), \kappa(R), \kappa(S)) = d^\alpha.$$

Es ist also $d^\alpha = d$ für alle $d \in K$, die von 0 und 1 verschieden sind. Es ist aber auch $0^\alpha = 0$ und $1^\alpha = 1$. Daher ist $\alpha = 1_K$, so dass κ projektiv ist. Damit ist alles bewiesen.

Das Semikolon in $DV(P,Q;R,S)$ soll andeuten, dass es Symmetrien gibt. So ist beispielsweise $DV(P,Q;R,S) = DV(Q,P;S,R)$. Hierauf werden wir aber nicht weiter eingehen. Gesagt sei nur, dass DV bei den 24 Permutationen der P, Q, R, S höchstens sechs verschiedene Werte annimmt.

6. Graßmannsche Mannigfaltigkeiten I

Es sei V ein Vektorraum des Ranges n über dem kommutativen Körper K. Die Menge $G_r(V)$ der Punkte von $\mathrm{L}(\bigwedge_K^r(V))$, die durch zerlegbare Vektoren aufgespannt werden, nennen wir *graßmannsche Mannigfaltigkeit* mit den Parametern n und r. Die Bilder von $G_r(V)$ unter der Kollineationsgruppe von $\mathrm{L}(\bigwedge_K^r(V))$ nennen wir ebenfalls *graßmannsche Mannigfaltigkeiten*. Zwei graßmannsche Mannigfaltigkeiten G in $\mathrm{L}(X)$ und H in $\mathrm{L}(Y)$ heißen *projektiv äquivalent*, falls es einen Isomorphismus σ von $\mathrm{L}(X)$ auf $\mathrm{L}(Y)$ gibt mit $\sigma(G) = H$.

Wie zuvor bezeichnen wir mit $\mathrm{UR}_r(V)$ die Menge der Unterräume des Ranges r von V. Ist $U \in \mathrm{UR}_r(V)$ und sind $u_1, \ldots, u_r$ und $v_1, \ldots, v_r$ Basen von U, so ist

$$(u_1 \wedge \ldots \wedge u_r)K = (v_1 \wedge \ldots \wedge v_r)K$$

nach 4.3 und nach 1.10 ist $u_1 \wedge \ldots \wedge u_r \neq 0$. Setzt man nun

$$\gamma(U) := (u_1 \wedge \ldots \wedge u_r)K,$$

so ist γ also wohldefiniert und überdies eine Abbildung von $\mathrm{UR}_r(V)$ in $G_r(V)$. Ist andererseits $(x_1 \wedge \ldots \wedge x_r)K$ ein Punkt von $G_r(V)$, so sind die x_i linear unabhängig und es ist

$$\gamma\big(\textstyle\sum_{i:=1}^r x_i K\big) = (x_1 \wedge \ldots \wedge x_r)K,$$

so dass γ auch surjektiv ist. Wir nennen γ *graßmannsche Abbildung* von $\mathrm{UR}_r(V)$ auf $G_r(V)$.

Sind X und Y Unterräume von V mit $X \leq Y$ und ist $\mathrm{Rg}_K(X) \leq r \leq \mathrm{Rg}_K(Y)$, so setzen wir

$$\mathrm{UR}_r(Y, X) := \{U \mid U \in \mathrm{UR}_r(V), X \leq U \leq Y\}.$$

Die wichtigste Eigenschaft von γ wird durch den folgenden Satz ausgedrückt.

6.1. Satz. *Es sei V ein Vektorraum des Ranges n über dem kommutativen Körper K. Ferner seien X und Y zwei Unterräume von V und es gelte $X \leq Y$. Setze $t := \mathrm{Rg}_K(X)$ und $s := \mathrm{Rg}_K(Y)$. Es sei $x_1, \ldots, x_t$ eine Basis von X. Ist dann $t \leq r \leq s$, so gibt es einen Monomorphismus η von $\bigwedge_K^{r-t}(Y/X)$ in $\bigwedge_K^r(V)$ mit*

$$\eta((y_1 + X) \wedge \ldots \wedge (y_{r-t} + X)) = x_1 \wedge \ldots \wedge x_t \wedge y_1 \wedge \ldots \wedge y_{r-t}$$

für alle $y_1, \ldots, y_{r-t} \in Y$. Setzt man

$$G := \{\gamma(U) \mid U \in \mathrm{UR}_r(Y, X)\},$$

so ist weiter $G = \eta(G_{s-t,r-t}(Y/X))$. Insbesondere ist G eine zu $G_{s-t,r-t}(Y/X)$ isomorphe Teilmannigfaltigkeit von $G_r(V)$. Die Punkte von G spannen einen Teilraum des Ranges $\binom{s-t}{r-t}$ auf.

Beweis. Sind $y_1 \ldots, y_{r-t} \in Y$, so setzen wir

$$\psi(y_1 + X, \ldots, y_{r-t} + X) := x_1 \wedge \ldots \wedge x_r \wedge y_1 \wedge \ldots \wedge y_{r-t}.$$

Ist $u \in X$, so ist

$$x_1 \wedge \ldots \wedge x_t \wedge u = 0.$$

Daher ist ψ wohldefiniert. Weil ψ banalerweise $(r-t)$-fach alternierend ist, gibt es eine lineare Abbildung η von $\bigwedge_K^{r-t}(Y/X)$ in $\bigwedge_K^r(V)$ mit

$$\eta((y_1 + X) \wedge \ldots \wedge (y_{r-t} + X)) = x_1 \wedge \ldots \wedge x_t \wedge y_1 \wedge \ldots \wedge y_{r-t}.$$

Mittels einer Basis $z_1 + X, \ldots, z_{s-t} + X$ von Y/X sieht man, dass η mindestens den Rang $\binom{s-t}{r-t}$ hat. Weil das Urbild aber diesen Rang hat, folgt, dass η ein Monomorphismus ist. Hieraus folgt wiederum, dass

$$H := \eta(G_{s-t,r-t}(Y/X))$$

eine zu $G_{s-t,r-t}(Y/X)$ isomorphe Teilmannigfaltigkeit von $G_r(V)$ ist. Ferner ist $H \subseteq G$. Es sei nun $P \in G$ und $U := \gamma^{-1}(P)$. Dann ist $X \leq U \leq Y$. Es gibt daher Elemente $y_1, \ldots, y_{r-t} \in Y$, so dass $x_1, \ldots, x_r, y_1, \ldots, y_{r-t}$ eine Basis von U ist. Wegen

$$\begin{aligned} P = \gamma(U) &= (x_1 \wedge \ldots \wedge x_t \wedge y_1 \wedge \ldots \wedge y_{r-t})K \\ &= \eta((y_1 + X) \wedge \ldots \wedge (y_{r-t} + X))K \end{aligned}$$

ist sogar $H = G$. Damit ist alles bewiesen.

Die Vektoren aus $\bigwedge_K^1(V)$ sind alle zerlegbar und nach 4.7 sind auch alle Vektoren aus $\bigwedge_K^{n-1}(V)$ zerlegbar, falls n der Rang von V ist. Hieraus folgt, dass $G_{n,1}(V)$ aus den Punkten von $\mathrm{L}(\bigwedge_K^1(V))$ und $G_{n,n-1}(V)$ aus den Punkten von $\mathrm{L}(\bigwedge_K^{n-1}(V))$ besteht. Aus diesen Bemerkungen folgen nun sofort die Korollare 6.2 und 6.3.

6.2. Korollar. *Es sei V ein Vektorraum des Ranges n über dem kommutativen Körper K. Ferner seien X und Y zwei Teilräume des Ranges $r-1$ und s von V und es gelte $X \leq Y$. Ist wieder*

$$G := \{\gamma(U) \mid U \in \mathrm{L}_r(Y, X)\},$$

so besteht G aus den Punkten eines Unterraumes W des Ranges $s - r + 1$. Überdies wird die Einschränkung γ_0 von γ auf $\mathrm{L}_r(Y, X)$ durch eine lineare Abbildung von Y/X auf W induziert.

6.3. Korollar. *Es sei V ein Vektorraum des Ranges n über dem kommutativen Körper K. Ferner seien X und Y zwei Teilräume des Ranges t und $r+1$ von V und es gelte $X \leq Y$. Dann besteht*

$$G := \{\gamma(U) \mid U \in \mathrm{UR}_r(Y, X))\}$$

aus den Punkten eines Unterraumes W des Ranges $r+1-t$. Überdies wird die Einschränkung γ_1 von γ auf $\mathrm{L}_r(Y, X)$ durch eine lineare Abbildung von Y/X auf W induziert.

Setzt man $s := n$ in 6.2, so folgt, dass $G_r(V)$ eine Schar S^I von Teilräumen des Ranges $n-r+1$ enthält. Setzt man $t := 0$ in 6.3, so sieht man, dass $G_r(V)$ auch eine Schar S^{II} von Teilräumen des Ranges $r+1$ enthält. Wir werden später sehen, dass alle Teilräume von $\mathrm{L}(\bigwedge_K^r(V))$, deren Punkte zu $G_r(V)$ gehören, in einem Raum aus $S^I \cup S^{II}$ enthalten sind.

6.4. Satz. *Es sei V ein Vektorraum endlichen Ranges über dem kommutativen Körper K. Ferner sei $U \in \mathrm{UR}_r(V)$ und $V = U \oplus C$. Ist dann S die Menge der Punkte der Form $(c \wedge u_1 \wedge \ldots \wedge u_{r-1})K$ mit $c \in C$ und $u_i \in U$, so ist S zur Segreschen Mannigfaltigkeit $S(C, U^*)$ projektiv äquivalent. Ist W ein erzeugender Raum der ersten Schar von S, so ist $\gamma(U) + W \in S^I$. Ist W ein erzeugender Raum der zweiten Schar von S, so ist $\gamma(U) + W \in S^{II}$.*

Beweis. Es sei ϵ die Inklusionsabbildung von U in $\bigwedge_K(U)$ und ι sei die Inklusionsabbildung von U in $V \leq \bigwedge_K(V)$. Dann ist $\iota(u) \wedge \iota(u) = u \wedge u = 0$ für alle $u \in U$. Es gibt also einen Algebrenhomomorphismus τ von $\bigwedge_K(U)$ in $\bigwedge_K(V)$ mit $\tau\epsilon(u) = \iota(u) = u$ für alle $u \in U$. Insbesondere ist

$$\tau((\epsilon(u_1) \wedge \ldots \wedge \epsilon(u_{r-1})) = \tau\epsilon(u_1) \wedge \ldots \wedge \tau\epsilon(u_{r-1}) = u_1 \wedge \ldots \wedge u_{r-1}.$$

Also ist $\tau(\bigwedge_K^{r-1}(U)) \leq \bigwedge_K^{r-1}(V)$. Da $\mathrm{Rg}_K(U) = r$ ist, sind die Elemente aus $\bigwedge_K^{r-1}(U)$ alle zerlegbar. Es sei $x \in \bigwedge_K^{r-1}(U)$ und es gelte $\tau(x) = 0$. Es gibt dann $u_1, \ldots, u_{r-1} \in U$ mit

$$x = \epsilon(u_1) \wedge \ldots \wedge \epsilon(u_{r-1}).$$

Es folgt

$$0 = \tau(\epsilon(u_1) \wedge \ldots \wedge \epsilon(u_{r-1}) = u_1 \wedge \ldots \wedge u_{r-1},$$

so dass die u_i linear abhängig sind. Dann sind aber auch die $\epsilon(u_i)$ linear abhängig, so dass

$$x = \epsilon(u_1) \wedge \ldots \wedge \epsilon(u_{r-1}) = 0$$

ist. Somit ist die Einschränkung von τ auf $\bigwedge_K^{r-1}(U)$ ein Monomorphismus von $\bigwedge_K^{r-1}(U)$ in $\bigwedge_K^{r-1}(V)$. Setze

$$\tilde{U} := \{u_1 \wedge \ldots \wedge u_{r-1} \mid u_i \in U\}.$$

Dann ist $\tilde{U}$ ein zu $\bigwedge_K^{r-1}(U)$ isomorpher Unterraum von $\bigwedge_K^{r-1}(V)$, wie gerade gezeigt.

Die durch

$$(u_1 \wedge \ldots \wedge u_{r-1})^* u := u_1 \wedge \ldots \wedge u_{r-1} \wedge u$$

definierte Abbildung $*$ ist eine lineare Abbildung von $\tilde{U}$ in U^*. Aus $(u_1 \wedge \ldots \wedge u_{r-1})^* = 0$ folgt, da $\mathrm{Rg}_K(U) = r$ ist, dass $u_1 \wedge \ldots \wedge u_{r-1} = 0$ ist. Daher ist $*$ injektiv. Schließlich folgt aus

$$\mathrm{Rg}_K(\tilde{U}) = \mathrm{Rg}_K(\textstyle\bigwedge_K^{r-1}(U)) = r = \mathrm{Rg}_K(U^*),$$

dass $*$ sogar bijektiv ist.

Die Abbildung

$$(c, (u_1 \wedge \ldots \wedge u_{r-1})^*) \to c \wedge u_1 \wedge \ldots \wedge u_{r-1}$$

ist eine bilineare Abbildung von $C \times U^*$ in $\bigwedge_K^r(V)$. Es gibt folglich eine lineare Abbildung σ von $C \otimes U^*$ in $\bigwedge_K^r(V)$ mit

$$\sigma(c \otimes (u_1 \wedge \ldots \wedge u_{r-1})^*) = c \wedge u_1 \wedge \ldots u_{r-1}.$$

Der von den $c \wedge u_1 \wedge \ldots \wedge u_{r-1}$ aufgespannte Unterraum X hat mindestens den Rang $(n-r)r$. Ist nämlich $c_1, \ldots, c_{n-r}$ eine Basis von C und $b_1, \ldots, b_r$ eine Basis von U, so ist wegen $U \cap C = \{0\}$ die Menge der r-Vektoren der Form

$$c_j \wedge b_1 \wedge \ldots \wedge b_{i-1} \wedge b_{i+1} \wedge \ldots \wedge b_r$$

nach Satz 1.7 linear unabhängig. Die Anzahl dieser Vektoren ist aber gleich $(n-r)r$. Weil X ein epimorphes Bild von $C \otimes U^*$ ist und weil der Rang dieses Raumes gleich $(n-r)r$ ist, folgt, dass der Rang von X gleich $(n-r)r$ ist. Dies hat wiederum zur Folge, dass σ ein Isomorphismus von $C \otimes U^*$ auf X ist. Offensichtlich gilt auch

$$\sigma(S(C, U^*)) = S.$$

Damit ist die erste Aussage des Satzes bewiesen.

Als nächstes zeigen wir, dass $\gamma(U) \cap X = \{0\}$ ist. Dazu nehmen wir an, dies sei nicht der Fall. Da $\gamma(U)$ ein Punkt ist, ist dann $\gamma(U) \leq X$, so dass es ein $c \in C$ und u_i in U gibt mit

$$\gamma(U) = (c \wedge u_1 \wedge \ldots \wedge u_{r-1})K.$$

Weil $c \wedge u_1 \wedge \ldots \wedge u_{r-1} \neq 0$ ist, sind die u_i linear unabhängig. Es gibt also ein $u_0 \in U$, so dass $u_0, \ldots, u_{r-1}$ eine Basis von U ist. Dann ist aber $\gamma(U) = (u_0 \wedge \ldots \wedge u_{r-1})K$. Es gibt also ein $k \in K^*$ mit

$$c \wedge u_1 \wedge \ldots \wedge u_{r-1} = (u_0 \wedge \ldots u_{r-1})k.$$

Es folgt

$$(c - u_0 k) \wedge u_1 \wedge \ldots u_{r-1} = 0,$$

so dass $c - u_0 k, u_1, \ldots, u_{r-1}$ linear abhängig sind. Weil die $u_1, \ldots, u_{r-1}$ linear unabhängig sind, folgt, dass $c - u_0 k$ von $u_1, \ldots, u_{r-1}$ linear abhängt. Dies hat schließlich $c \in U$ zur Folge. Damit erhalten wir den Widerspruch

$$0 \neq c \in C \cap U = \{0\}.$$

Also ist doch $\gamma(U) \cap X = \{0\}$.

Es sei nun W ein Raum der ersten Schar von S. Es gibt dann $u_1, \ldots, u_{r-1} \in U$ mit

$$W = \{c \wedge u_1 \wedge \ldots \wedge u_{r-1} \mid c \in C\}.$$

Es gibt ferner ein u_0, so dass $u_0, u_1, \ldots, u_{r-1}$ eine Basis von U ist. Es folgt

$$\gamma(U) = \{(u_0 k) \wedge u_1 \wedge \ldots \wedge u_{r-1} \mid k \in K\}.$$

Somit ist

$$\gamma(U) + W = \{(u_0 k + c) \wedge u_1 \wedge \ldots \wedge u_{r-1} \mid k \in K, c \in C\}.$$

Hieraus folgt, dass $\mathrm{Rg}_K(\gamma(U) + W) = n - r + 1$ ist. Ferner ist klar, dass die Punkte von $\gamma(U) + W$ gerade den Unterräumen vom Rang r entsprechen, die $u_1, \ldots, u_r$ enthalten. Also ist $\gamma(U) + W \in S^I$.

Es sei nun W ein Raum der zweiten Schar von S. Es gibt dann ein $c \in C$ mit $c \neq 0$ und

$$W = \{c \wedge u_1 \wedge \ldots \wedge u_{r-1} \mid u_i \in U\}.$$

Es sei $v_0, \ldots, v_{r-1}$ eine Basis von U. Dann ist $\gamma(U) = (v_0 \wedge \ldots \wedge v_{r-1})K$. Es sei P ein Punkt von $\gamma(U) + W$ und es sei $P = xK$. Es gibt dann ein $k \in K$ und $u_1, \ldots, u_{r-1} \in U$ mit

$$x = (v_0 k) \wedge v_1 \wedge \ldots \wedge v_{r-1} + c \wedge u_1 \wedge \ldots \wedge u_{r-1}.$$

Wir dürfen annehmen, dass $u_1 \wedge \ldots \wedge u_{r-1} \neq 0$ ist. Dann gibt es ein u_0, so dass $u_0, u_1, \ldots, u_{r-1}$ eine Basis von U ist. Es folgt $\gamma(U) = (u_0 \wedge \ldots \wedge u_{r-1})K$, so dass es ein $l \in K$ gibt mit

$$\begin{aligned} x &= (u_0 l) \wedge u_1 \wedge \ldots \wedge u_{r-1} + c \wedge u_1 \wedge \ldots \wedge u_{r-1} \\ &= (u_0 l + c) \wedge u_1 \wedge \ldots \wedge u_{r-1}. \end{aligned}$$

Hieraus folgt

$$\gamma^{-1}(P) = V_x \leq U \oplus cK.$$

Es sei umgekehrt X ein Unterraum des Ranges r von $U \oplus cK$. Ist $X = U$, so ist $\gamma(X) \leq \gamma(U) + W$. Es sei also $X \neq U$. Dann ist $\mathrm{Rg}_K(X \cap U) = r - 1$. Es sei $u_1, \ldots, u_{r-1}$ eine Basis von $U \cap X$ und $v_0, u_1, \ldots, u_{r-1}$ eine Basis von X. Es gibt dann ein $u \in U$ und ein $k \in K$ mit $v = u + ck$. Es folgt

$$v \wedge u_1 \wedge \ldots \wedge u_{r-1} = u \wedge u_1 \wedge \ldots \wedge u_{r-1} + (c \wedge u_1 \wedge \ldots \wedge u_{r-1})k.$$

Folglich ist $\gamma(X) \leq \gamma(U) + W$. Damit ist gezeigt, dass die Punkte von $\gamma(U) + W$ gerade die Bilder der Unterräume des Ranges r von $U \oplus cK$ sind. Folglich ist $\gamma(U) + W \in S^{II}$. Damit ist alles bewiesen.

Mit $S_{\gamma(U)}$ bezeichnen wir die Menge der Räume $\gamma(U) + W$ mit $W \in E_1 \cup E_2$, wobei E_i die $i$te Schar von Erzeugenden von S ist. Wir nennen $S_\gamma(U)$ *Segreschen Kegel mit der Spitze* $\gamma(U)$ von $G_r(V)$. Den von den Räumen aus $S_{\gamma(U)}$ aufgespannte Unterraum bezeichnen wir mit $T_{\gamma(U)}$ und nennen ihn *Tangentialraum* von $G_r(V)$ in $\gamma(U)$. Wie der Beweis von 6.4 zeigt, gilt

6.5. Korollar. *Es ist* $\mathrm{Rg}_K(T_{\gamma(U)}) = (n - r)r + 1$.

6.6. Satz. *Es sei V ein Vektorraum des Ranges n über dem kommutativen Körper K. Ist U ein Unterraum von $\bigwedge_K^r(V)$, dessen Punkte alle in $G_r(V)$ liegen, so ist U Unterraum eines Raumes aus $S^I \cup S^{II}$.*

Beweis. Es seien P und Q zwei verschiedene Punkte von U. Ferner sei $P = (u_1 \wedge \ldots \wedge u_r)K$ und $Q = (v_1 \wedge \ldots \wedge v_r)K$. Weil P und Q verschieden sind, sind $u_1 \wedge \ldots \wedge u_r$ und $v_1 \wedge \ldots \wedge v_r$ linear unabhängig. Wegen $P + Q \leq U$ und weil die Punkte von U alle zu $G_r(V)$ gehören gibt es $w_1, \ldots, w_r$ mit

$$u_1 \wedge \ldots \wedge u_r + v_1 \wedge \ldots \wedge v_r = w_1 \wedge \ldots \wedge w_r.$$

Überdies ist $w_1 \wedge \ldots \wedge w_r \neq 0$, da $u_1 \wedge \ldots \wedge u_r$ und $v_1 \wedge \ldots \wedge v_r$ linear unabhängig sind. Schließlich folgt, dass $V_{w_1 \wedge \ldots \wedge w_r} \neq V_{v_1 \wedge \ldots \wedge v_r}$ ist. Wir dürfen daher oBdA annehmen, dass $w_1 \notin V_{v_1 \wedge \ldots \wedge v_r}$ ist. Nun ist

$$0 = w_1 \wedge \ldots \wedge w_r \wedge w_1 = u_1 \wedge \ldots \wedge u_r \wedge w_1 + v_1 \wedge \ldots \wedge v_r \wedge w_1$$

und daher

$$u_1 \wedge \ldots \wedge u_r \wedge w_1 = -v_1 \wedge \ldots \wedge v_r \wedge w_1.$$

Setze $y := u_1 \wedge \ldots \wedge u_r \wedge w_1$. Aus der gerade bewiesenen Gleichung folgt dann, da $w_1 \notin V_{v_1 \wedge \ldots \wedge v_r}$ gilt, dass $y \neq 0$ ist. Nun ist

$$y \wedge u_i = 0 = y \wedge v_i$$

für alle i. Daher ist

$$V_{u_1 \wedge \ldots \wedge u_r} \leq V_y$$

und

$$V_{v_1 \wedge \ldots \wedge v_r} \leq V_y.$$

Weil $\mathrm{Rg}_K(V_y) = r + 1$ ist, folgt, dass $P + Q$ in einem Raum aus S^{II} liegt, da ja $\gamma(V_{u_1 \wedge \ldots \wedge u_r}) = P$ und $\gamma(V_{v_1 \wedge \ldots \wedge v_r}) = Q$ ist. Weil $\mathrm{Rg}_K(V_y) = r + 1$ ist folgt,

dass $\mathrm{Rg}_K(V_{u_1\wedge\ldots\wedge u_r} \cap V_{v_1\wedge\ldots\wedge v_r}) = r-1$ ist. Daher liegt $P+Q$ auch in einem Teilraum aus S^I. Die beiden Räume aus $S^I \cup S^{II}$ gehören zum Segreschen Kegel S_P mit der Spitze P. Hieraus folgt, falls X der von der zu P gehörenden Segreschen Mannigfaltigkeit S aufgespannte Raum ist, dass $U \cap X$ ganz in S liegt. Aus VI.3.9 und 6.4 folgt nun die Behauptung.

6.7. Satz. *Es sei V ein Vektorraum über dem kommutativen Körper K und der Rang von V sei endlich. Sind U, $U' \in \mathrm{UR}_r(V)$, so sind äquivalent:*
a) *Es ist* $\mathrm{Rg}_K(U+U') = r+1$.
b) *Es ist* $\mathrm{Rg}_K(U\cap U') = r-1$.
c) *Es ist $\gamma(U) \neq \gamma(U')$ und alle Punkte von $\gamma(U)+\gamma(U')$ liegen in $G_r(V)$.*

Beweis. Es ist

$$\mathrm{Rg}_K(U+U') + \mathrm{Rg}_K(U\cap U') = \mathrm{Rg}_K(U) + \mathrm{Rg}_K(U') = 2r.$$

Hieraus folgt, dass a) und b) äquivalent sind.

Aus a) und b) zusammen folgt einmal $\gamma(U) \neq \gamma(U')$ und mit 6.1 weiterhin, dass

$$\gamma(U), \gamma(U') \in G \cong G_1((U+U')/(U\cap U'))$$

ist. Dies besagt, dass $\gamma(U)$ und $\gamma(U')$ auf einer Geraden liegen, deren Punkte alle zu $G_r(V)$ gehören.

Aus c) folgen, wie wir beim Beweise von 6.6 gesehen haben, a) und b). Damit ist alles gezeigt.

6.8. Satz. *Es sei V ein Vektorraum des Ranges n über dem kommutativen Körper K. Ferner seien X und Y Unterräume des Ranges $r-1$ bzw. $r+1$ von V. Sind dann P, Q, R, S vier verschiedene Unterräume des Ranges r von Y, die X enthalten, und ist γ die graßmannsche Abbildung von $\mathrm{UR}_r(V)$ auf $G_r(V)$, so gilt*

$$DV(P,Q;R,S) = DV(\gamma(P),\gamma(Q);\gamma(R),\gamma(S)).$$

Sind umgekehrt P', Q', R' und S' vier verschiedene, kollineare Punkte von $G_r(V)$, so ist

$$DV(\gamma^{-1}(P'),\gamma^{-1}(Q');\gamma^{-1}(R'),\gamma^{-1}(S')) = DV(P',Q';R',S').$$

Beweis. Es sei $u_1, \ldots, u_{r-1}$ eine Basis von X. Ferner sei $d := DV(P,Q;R,S)$. Es gibt Vektoren p und q mit $P = X+pK$, $Q = X+qK$, $R = X+(p+q)K$ und $S = X+(p+qd)K$. Hieraus folgt

$$\begin{aligned}
\gamma(P) &= (u_1 \wedge \ldots \wedge u_{r-1} \wedge p)K\\
\gamma(Q) &= (u_1 \wedge \ldots \wedge u_{r-1} \wedge q)K\\
\gamma(R) &= (u_1 \wedge \ldots \wedge u_{r-1} \wedge (p+q))K\\
\gamma(S) &= (u_1 \wedge \ldots \wedge u_{r-1} \wedge (p+qd))K.
\end{aligned}$$

Setzt man

$$\begin{aligned}
p' &:= u_1 \wedge \ldots \wedge u_{r-1} \wedge p\\
q' &:= u_1 \wedge \ldots \wedge u_{r-1} \wedge q,
\end{aligned}$$

so ist also $\gamma(P) = p'K$, $\gamma(Q) = q'K$, $\gamma(R) = (p' + q')K$ und $\gamma(S) = (p' + q'd)K$. Also ist

$$DV(\gamma(P), \gamma(Q); \gamma(R), \gamma(S)) = d.$$

Dass γ^{-1} ebenfalls das Doppelverhältnis invariant lässt, beweist sich ebenso einfach.

6.9. Satz. *Es sei V ein Vektorraum des Ranges n über dem kommutativen Körper K. Ferner sei γ die graßmannsche Abbildung von $\mathrm{UR}_r(V)$ auf $G_r(V)$ und δ sei die graßmannsche Abbildung von $\mathrm{UR}_s(V)$ auf $G_s(V)$. Ist κ ein Isomorphismus von $\mathrm{L}(\bigwedge_K^r(V))$ auf $\mathrm{L}(\bigwedge_K^s(V))$, der $G_r(V)$ auf $G_s(V)$ abbildet, so gibt es eine Kollineation oder eine Korrelation λ von $\mathrm{L}(V)$ mit $\lambda(U) = \delta^{-1}\kappa\gamma(U)$ für alle $U \in \mathrm{UR}_r(V)$. Ist λ eine Kollineation, so ist $r = s$, und ist λ eine Korrelation, so ist $r + s = n$. Genau dann ist κ projektiv, wenn λ projektiv ist.*

Beweis. Es seien U und U' benachbarte Unterräume des Ranges r. Dann ist $\mathrm{Rg}_K(U + U') = r + 1$, so dass nach 6.7 alle Punkte von $\gamma(U) + \gamma(U')$ in $G_r(V)$ liegen. Daher liegen alle Punkte von $\kappa\gamma(U) + \kappa\gamma(U')$ in $G_s(V)$. Nach 6.7 sind folglich auch $\delta^{-1}\kappa\gamma(U)$ und $\delta^{-1}\kappa\gamma(U')$ benachbart, so dass die Existenz von λ aus dem Satz von Chow (Satz I.8.4) folgt, wie auch die Aussage über r und s.

Weil es Geraden gibt, deren Punkte allesamt in $G_r(V)$ liegen, folgt die letzte Behauptung aus den Sätzen 6.8 und 5.2.

6.10. Korollar. *Es sei V ein Vektorraum des Ranges n über dem kommutativen Körper K. Genau dann sind $G_r(V)$ und $G_s(V)$ projektiv äquivalent, wenn $r = s$ oder wenn $r + s = n$ ist.*

Beweis. Es ist aufgrund von 6.9 nur noch zu zeigen, dass $G_r(V)$ und $G_s(V)$ projektiv äquivalent sind, wenn $r + s = n$ ist. Dies folgt aber aus 3.3 und 4.6, wenn man nur noch V mit V^* über eine Basis von V und deren Dualbasis von V^* identifiziert, was ja wegen der Kommutativität von K möglich ist.

6.11. Satz. *Es sei V ein Vektorraum des Ranges n über dem kommutativen Körper K. Der Monomorphismus $\sigma \to \sigma_{\#r}$ induziert einen Monomorphismus von $PGL(V)$ auf eine Untergruppe $\Gamma_r^0(V)$ des Stabilisators $\Gamma_r(V)$ von $G_r(V)$ in $PGL(\bigwedge_K^r(V))$. Es gilt:*
a) *Ist $n \neq 2r$, so ist $\Gamma_r(V) = \Gamma_r^0(V)$.*
b) *Ist $n = 2r$, so ist $|\Gamma_r(V) : \Gamma_r^0(V)| = 2$.*

Beweis. Aus Satz 1.11 folgt, dass die Abbildung

$$\sigma \to \sigma_{\#r}$$

einen Homomorphismus von $PGL(V)$ auf eine Untergruppe $\Gamma_r^0(V)$ von $\Gamma_r(V)$ induziert. Lässt $\sigma_{\#r}$ alle Punkte von $G_r(V)$ fest, so ist also

$$\sigma(v_1) \wedge \ldots \wedge \sigma(v_r) = \sigma_{\#r}(v_1 \wedge \ldots \wedge v_r) = (v_1 \wedge \ldots \wedge v_r)k$$

für alle $(v_1, \ldots, v_r) \in V^r$, wobei k von den v_i abhängt. Es folgt, dass σ alle Unterräume des Ranges r von V festlässt, so dass die Abbildung σ in $\mathrm{L}(V)$ die

Identität induziert. Dies zeigt, dass die Abbildung $\sigma \to \sigma_{\#r}$ einen Isomorphismus von $PGL(V)$ auf $\Gamma_r^0(V)$ induziert.

Nach 6.9 gibt es zu jedem $\kappa \in \Gamma_r(V)$ eine Kollineation oder Korrelation λ von $\mathrm{L}(V)$ mit

$$\lambda(U) = \gamma^{-1}\kappa\gamma(U)$$

für alle $U \in \mathrm{UR}_r(V)$. Es sei $\Gamma_r^1(V)$ die Untergruppe aller $\kappa \in \Gamma_r(V)$, für die λ eine Kollineation ist. Es sei $U = \bigoplus_{i:=1}^r u_i K$ und $\kappa \in \Gamma_r^1(V)$. Schließlich sei $\lambda \in GL(V)$ und λ induziere die zu κ gehörende Kollineation in $\mathrm{L}(V)$, die wir ebenfalls mit λ bezeichnen. Dann ist

$$\gamma\lambda(U) = (\lambda(u_1) \wedge \ldots \wedge \lambda(u_r))K = \lambda_{\#r}(u_1 \wedge \ldots \wedge u_r)K = \lambda_{\#r}\gamma(U).$$

Somit ist $\gamma\lambda = \lambda_{\#r}\gamma$, dh.,

$$\gamma^{-1}\kappa\gamma = \lambda = \gamma^{-1}\lambda_{\#r}\gamma,$$

so dass $\kappa = \lambda_{\#r}$ ist. Folglich ist $\Gamma_r^1(V) = \Gamma_r^0(V)$.

a) In diesem Falle ist $\Gamma_r^1(V) = \Gamma_r(V)$ und damit $\Gamma_r^0(V) = \Gamma_r(V)$.

b) Weil das Produkt zweier Korrelationen eine Kollineation ist, ist

$$|\Gamma_r(V) : \Gamma_r^0| = |\Gamma_r(V) : \Gamma_r^1(V)| \leq 2.$$

Die Kollineationen aus $\Gamma_r^0(V)$ lassen die Scharen S^I und S^{II} je für sich invariant. Lässt man r in 6.10 die Rollen von r und von s spielen, was wegen $n = 2r$ ja möglich ist, so sieht man, dass es auch Kollineationen in $\Gamma_r(V)$ gibt, die die Scharen S^I und S^{II} vertauschen. Damit ist alles bewiesen.

7. Graßmannsche Mannigfaltigkeiten II

Wir haben in Abschnitt 4 Kriterien für die Zerlegbarkeit von r-Vektoren gegeben. In diesem Abschnitt werden wir nun eine geometrische Deutung dieser Kriterien geben. Sie lassen sich nämlich dahingehend interpretieren, dass sich jede graßmannsche Mannigfaltigkeit als Schnitt von endlich vielen Quadriken darstellen lässt.

Es sei V ein Vektorraum über dem kommutativen Körper K und f sei das in Satz 2.12 beschriebene Skalarprodukt auf $\bigwedge_K(V^*) \times \bigwedge_K(V)$. Ist x ein zerlegbarer $(n-r-1)$-Vektor und w eine zerlegbare $(r-1)$-Form, so definieren wir die Abbildung $Q_{w,x}$ von $\bigwedge_K^r(V)$ in K durch

$$Q_{w,x}(z) := f(w, z \vee (z \wedge x)).$$

Banal ist, dass $Q_{w,x}(zk) = Q_{w,x}(z)k^2$ ist. Langweilige Routinerechnungen zeigen, wobei man auf die Definition von $\vee$ vor Satz 4.8 zurückgreifen muss, dass

$$Q_{w,x}(z+z') = Q_{w,x}(z) + Q_{w,x}(z') + f(w, z \vee (z' \wedge x)) + f(w, z' \vee (z \wedge x))$$

ist. Ebensolche Routinerechnungen zeigen, dass die Abbildung

$$(z, z') \to f(w, z \vee (z' \wedge x)) + f(w, z' \vee (z \wedge x))$$

bilinear ist. Daher ist $Q_{w,x}$ eine quadratische Form.

7.1. Satz. *Ist $\sigma \in GL(V)$, ist x ein zerlegbarer $(n-r-1)$-Vektor und w eine zerlegbare $(r-1)$-Form, ist schließlich $\bar{x} = \sigma^{-1}_{\#(n-r-1)}(x)$ und $\bar{w} = \sigma^*_{\#(r-1)}(w)$, so sind $Q_{w,x}$ und $Q_{\bar{w},\bar{x}}$ projektiv äquivalent.*

Beweis. Nach 3.5 gibt es ein $k \in K^*$ mit $\varphi\sigma_{\#r}\mu_k = \sigma^{*-1}_{\#(n-r)}\varphi$. Benutzt man dies und 1.11 d), so folgt:

$$\begin{aligned}\varphi(\sigma_{\#r}(z)) \vee (\sigma_{\#r}(z) \wedge x) &= \varphi(\sigma_{\#r}(z)) \wedge \varphi(\sigma_{\#r}(z) \wedge \sigma_{\#(n-r-1)}(\bar{x}))\\ &= \sigma^{*-1}_{\#(n-r)}\varphi(z) \wedge \sigma^{*-1}\varphi(\bar{x})k^{-2}\\ &= \sigma^{*-1}_{\#(n-r+1)}(\varphi(z) \wedge \varphi(z \wedge \bar{x}))k^{-2}.\end{aligned}$$

Also ist

$$\sigma_{\#r}(z) \vee (\sigma_{\#r} \wedge x) = \sigma^{*-1}(\varphi(z) \wedge \varphi(z \wedge \bar{x}))k^{-2}.$$

Nach 3.5 gilt auch $\varphi\sigma_{\#(r-1)}\mu_k = \sigma_{\#(n-r+1)}\varphi$, da k von r unabhängig ist. Also ist

$$\sigma_{\#r}(z) \vee (\sigma_{\#r}(z) \wedge x) = \sigma_{\#(r-1)}(z \vee (z \wedge \bar{x}))k^{-1}.$$

Hieraus folgt schließlich, dass

$$Q_{w,x}(\sigma_{\#r}(z)) = f(w, z \vee (z \wedge \bar{x}))k^{-1} = k^{-1}Q_{\bar{w},\bar{x}}(z)$$

ist. Folglich sind $Q_{w,x}$ und $Q_{\bar{w},\bar{x}}$ projektiv äquivalent.

Für den Rest des Abschnitts vereinbaren wir das folgende. Es sei V ein Vektorraum des Ranges n über dem kommutativen Körper K. Es sei $x_1, \ldots, x_n$ eine Basis von V und $y = x_1 \wedge \ldots \wedge x_n$. Ferner sei $x_1^*, \ldots, x_n^*$ die zu $x_1, \ldots, x_n$ duale Basis von V^*. Mit $(x_I \mid I \subseteq \{1, \ldots, n\})$ bzw. $(x_J^* \mid J \subseteq \{1, \ldots, n\})$ seien die entsprechenden Basen von $\bigwedge_K(V)$ bzw. $\bigwedge_K(V^*)$ bezeichnet. Statt $Q_{x_J^*, x_I}$ schreiben wir $Q_{J,I}$.

7.2. Satz. *Es seien I, I', J, J' Teilmengen von $\{1, \ldots, n\}$. Gilt $|I| = n-r-1 = |I'|$ und $|J| = r-1 = |J'|$ sowie $|I \cap J| = |I' \cap J'|$, so sind $Q_{J,I}$ und $Q_{J',I'}$ projektiv äquivalent.*

Beweis. Aufgrund der Annahme über I, J, I' und J' gibt es ein $\pi \in S_n$ mit $\pi(I) = I'$ und $\pi(J) = J'$. Ferner gibt es genau ein $\sigma \in GL(V)$ mit $\sigma(x_i) = x_{\pi^{-1}(i)}$ für alle i. Dann ist $\sigma^{-1}(x_i) = x_{\pi(i)}$ und $\sigma^*(x_j^*) = x^*_{\pi(j)}$, wie man leicht nachrechnet. Es folgt $\sigma_{\#n}(y) = \operatorname{sgn}(\pi)y$ und $\sigma_{\#(n-r-1)}(x_I) = \epsilon_1 x_{I'}$ und $\sigma^*_{\#(r-1)}(x_J^*) = \epsilon_2 x^*_{J'}$, wobei $\epsilon_i = \pm 1$ ist. Hieraus folgt, wie der Beweis von 7.1 zeigt, dass

$$Q_{J,I}(\sigma_{\#r}(z)) = \epsilon_1\epsilon_2\sigma(\pi)Q_{J',I'}(z)$$

ist. Damit ist der Satz bewiesen.

Es sei $z \in \bigwedge_K^r(V)$. Dann ist $z = \sum_{|L|=r} x_L a_L$. Nach 3.4 ist daher

$$\varphi(z) = \sum_{|L|=r} x_{L^c}^* a_L \prod_{\lambda \in L, \mu \in L^c} \langle \mu, \lambda \rangle.$$

Dabei ist L^c das Komplement von L in $\{1, \ldots, n\}$. Ferner ist

$$z \wedge x_I = \sum_{|L|=r} x_{L \cup I} a_L \prod_{\alpha \in L, \beta \in I} \langle \alpha, \beta \rangle,$$

und daher

$$\varphi(z \wedge x_I) = \sum_{|L|=r} x_{L^c \cap I^c}^* a_L \prod_{\alpha \in L, \beta \in I} \langle \alpha, \beta \rangle \prod_{\gamma \in L \cup I, \delta \in L^c \cap I^c} \langle \delta, \gamma \rangle.$$

Somit ist

$$\varphi(z) \wedge \varphi(z \wedge x_I) = \sum_{|L|=r} \sum_{|M|=r} x_{L^c \cup (M^c \cap I)}^* a_L a_M B_{L,M},$$

wobei

$$B_{L,M} = \prod_{\lambda \in L, \mu \in L^c} \langle \mu, \lambda \rangle \prod_{\alpha \in M, \beta \in I} \langle \alpha, \beta \rangle \prod_{\gamma \in M \cup I, \delta \in M^c \cap I^c} \langle \gamma, \delta \rangle \prod_{\epsilon \in L^c, \zeta \in M^c \cap I^c} \langle \epsilon, \zeta \rangle$$

ist. Schließlich ist

$$z \vee (z \wedge x_I) = \sum_{|L|=r} \sum_{|M|=r} x_{L \cap (M \cup I)} a_L a_M B_{L,M} \prod_{\substack{\eta \in L \cap (M \cup I) \\ \theta \in L^c \cup (M^c \cap I^c)}} \langle \theta, \eta \rangle.$$

Nun sind $(x_R \mid R)$ und $(x_S^* \mid S)$ duale Basen. Folglich ist

$$f(x_{L \cap (M \cup I)}, x_J^*) = 0,$$

falls $L \cap (M \cup I) \neq J$ ist. Also ist

$$Q_{J,I} = \epsilon_J \sum_{|L|=|M|=r, L \cap (M \cup I) = J} a_L a_M B_{L,M}$$

mit

$$\epsilon_J = \prod_{\eta \in J, \theta \in J^c} \langle \theta, \eta \rangle.$$

Wir wollen sehen, wie wir den Ausdruck für $Q_{J,I}$ noch vereinfachen können. Dazu fragen wir zunächst, wann unter der Nebenbedingung $L \cap (M \cup I) = J$ der Koeffizient $B_{L,M} \neq 0$ ist. Dazu ist, wie der eben etablierte Ausdruck für $B_{L,M}$ zeigt, hinreichend und notwendig, dass $M \cap I = \emptyset$ und $L \cup M \cup I = \{1, \ldots, n\}$ ist. Aus $M \cap I = \emptyset$ folgt, dass

$$|M \cup I| = r + n - r - 1 = n - 1$$

ist. Es gibt also ein i_M mit

$$M \cup I \cup \{i_M\} = \{1, \dots, n\}$$

und

$$i_M \notin M \cup I.$$

Aus $L \cup M \cup I = \{1, \dots, n\}$ folgt, dass $i_M \in L$ ist, und $L \cap (M \cup I) = J$ und $i_M \notin M \cup I$ implizieren, dass $i_M \notin J$ ist. Also ist $|J \cup \{i_M\}| = r$. Nun ist $L \subseteq J \cup \{i_M\}$ und $|L| = r$, so dass $L = J \cup \{i_M\}$ ist. Wir setzen nun

$$(i) \qquad C_{L,M} := \prod_{\alpha \in M, \beta \in I} \langle \alpha, \beta \rangle \prod_{\gamma \in L^c} \langle \gamma, i_M \rangle.$$

Dann gilt

7.3. Satz. *Es sei $|I| = n - r - 1$ und $|J| = r - 1$. Dann ist*

$$Q_{J,I}(z) = \epsilon_J \epsilon'_J \sum_{|M|=r, M \cap I = \emptyset, J \subseteq M \cup I} a_M a_{J \cup \{i_M\}} C_{J \cup \{i_M\}, M}.$$

Dabei ist i_M das Element aus der Gleichung $M \cup I \cup \{i_M\} = \{1, \dots, n\}$. Ferner ist

$$\epsilon_J = \prod_{\eta \in J, \delta \in J^c} \langle \theta, \eta \rangle \qquad \text{und} \qquad \epsilon'_J = (-1)^{nr + \frac{1}{2} r(r-1) + \Sigma J - 1},$$

wobei ΣX abkürzend für $\sum_{y \in X} y$ steht.

Beweis. Setze $L := J \cup \{i_M\}$. Es sei $L = \{\lambda_1, \dots, \lambda_r\}$ mit $\lambda_1 < \dots < \lambda_r$. Dann ist

$$\begin{aligned}\prod_{\lambda \in L,\, \mu \in L^c} \langle \mu, \lambda \rangle = \prod_{i:=1}^{r} \prod_{\mu \in L^c} \langle \mu, \lambda_i \rangle &= \prod_{i:=1}^{r} (-1)^{n - \lambda_i - (r-i)} \\ &= (-1)^{nr + \frac{1}{2} r(r-1) + i_M + \Sigma J}.\end{aligned}$$

Ferner ist $M^c \cap I^c = \{i_M\}$, so dass

$$\prod_{\gamma \in M \cup I, \delta \in M^c \cap I^c} \langle \delta, \gamma \rangle = \sum_{\gamma \in M \cup I} \langle i_M, \gamma \rangle = (-1)^{i_M - 1}$$

ist. Schließlich ist

$$\prod_{\epsilon \in L^c, \zeta \in M^c \cap I^c} \langle \epsilon, \zeta \rangle = \prod_{\epsilon \in L^c} \langle \epsilon, i_M \rangle.$$

Daher ist

$$B_{L,M} = (-1)^{mr + \frac{1}{2} r(r-1) + i_M + \Sigma J + i_M - 1} C_{L,M} = \epsilon'_J C_{L,M}.$$

Hieraus folgt schließlich die Behauptung.

7.4. Satz. *Ist $I \cap J = \emptyset$, so ist $Q_{J,I} = 0$.*

Beweis. Aufgrund von 7.2 dürfen wir annehmen, dass

$$I = \{1, \ldots, n - r - 1\}$$

und

$$J := \{n - r, \ldots, n - 2\}$$

ist. Aus $J \subseteq M \cup I$ und $I \cap J = \emptyset$ folgt, dass $J \subseteq M$ ist. Für M gibt es daher nur die beiden Möglichkeiten $M_1 = J \cup \{n-1\}$ und $M_2 = J \cup \{n\}$. Dann ist aber

$$L_1 = J \cup \{n\} = M_2$$

und

$$L_2 = J \cup \{n-1\} = M_1.$$

Nun ist $\beta < \alpha$, falls $\beta \in I$ und $\alpha \in M_i$ ist. Also ist

$$\prod_{\alpha \in M_1, \beta \in I} \langle \alpha, \beta \rangle = \prod_{\alpha \in M_2, \beta \in I} \langle \alpha, \beta \rangle.$$

Diesen gemeinsamen Wert nennen wir ϵ.

Es ist $i_{M_1} = n \in L_1$ und daher

$$\prod_{\gamma \in L_1^c} \langle \gamma, i_{M_1} \rangle = 1.$$

Ferner ist $i_{M_2} = n - 1 \in L_2$ und $n \in L_2^c$. Daher ist

$$\prod_{\gamma \in L_2^c} \langle \gamma, i_{M_2} \rangle = -1.$$

Somit ist

$$B_{L_1, M_1} = \epsilon = -B_{L_2, M_2}.$$

Hieraus folgt schließlich, dass

$$Q_{J,I}(z) = \epsilon_J \epsilon'_J \epsilon (a_{L_1} a_{M_1} - a_{L_2} a_{M_2}) = \epsilon_J \epsilon'_J \epsilon (a_{M_2} a_{M_1} - a_{M_1} a_{M_2}) = 0$$

ist. Damit ist 7.4 bewiesen.

Wir sind nun in der Lage, den folgenden Satz zu beweisen.

7.5. Satz. *Ist V ein Vektorraum des Ranges n über dem kommutativen Körper K, so ist $G_r(V)$ Schnitt von*

$$\binom{n}{r+1}\left[\binom{n}{r-1} - \binom{r+1}{r-1}\right]$$

Quadriken in $\mathrm{L}(\bigwedge_K^r(V))$.

Beweis. Nach 4.8 ist $z \in \bigwedge_K^r(V)$ genau dann zerlegbar, wenn für alle zerlegbaren $(n-r-1)$-Vektoren x die Gleichung $z \vee (z \wedge x) = 0$ gilt. Dies ist natürlich

genau dann der Fall, wenn $z \vee (z \wedge x_I) = 0$ für alle $(n-r-1)$-Teilmengen I gilt. Nun ist $z \vee (z \wedge x_I)$ ein $(r-1)$-Vektor. Also ist $z \vee (z \wedge x_J)$ genau dann gleich Null, wenn

$$Q_{J,I}(z) = 0$$

für alle I mit $|I| = r-1$ ist. Es folgt, dass $G_r(V)$ Schnitt der Quadriken zu den

$$\binom{n}{n-r-1}\binom{n}{r-1} = \binom{n}{r+1}\binom{n}{r-1}$$

quadratischen Formen $Q_{J,I}$ ist. Von diesen tragen aber nach 7.4 diejenigen zu dem Schnitt nichts bei, für die $I \cap J = \emptyset$ ist. Deren Anzahl ist

$$\binom{n}{n-r-1}\binom{r+1}{r-1} = \binom{n}{r+1}\binom{r+1}{r-1}.$$

Hieraus folgt die Behauptung.[5]

Wir betrachten den Spezialfall $n = 4$, $r = 2$, der schon von Plücker untersucht wurde. In diesem Falle ist $n - r - 1 = 1 = r - 1$. Hier sind also die quadratischen Formen $Q_{\{k\},\{k\}}$ für $k := 1, \ldots, 4$ zu betrachten. Berechnet man sie mit Hilfe von 7.3, so erhält man, wobei der unwesentliche Faktor $\epsilon_J \epsilon'_J$ nicht berücksichtigt ist,

$$\begin{aligned}
Q_{1,1}(z) &= a_{12}a_{34} - a_{13}a_{24} + a_{14}a_{23}\\
Q_{2,2}(z) &= a_{12}a_{34} - a_{24}a_{13} + a_{23}a_{14}\\
Q_{3,3}(z) &= a_{34}a_{12} - a_{13}a_{24} + a_{23}a_{14}\\
Q_{4,4}(z) &= a_{34}a_{12} - a_{24}a_{13} + a_{14}a_{23}.
\end{aligned}$$

Die vier Quadriken, die uns Satz 7.5 liefert, sind also nicht voneinander verschieden. Dies notieren wir als

7.6. Satz. *Ist V ein Vektorraum des Ranges 4 über dem kommutativen Körper K, so ist $G_2(V)$ eine Quadrik, die durch die Form*

$$Q(z) := a_{12}a_{34} - a_{13}a_{24} + a_{14}a_{23}$$

dargestellt wird. Sie ist von maximalem Index.

Man nennt $G_2(V)$ *Plückerquadrik*, falls $\mathrm{Rg}_K(V) = 4$ ist.

Wie der Fall der Plückerquadrik zeigt, kann es sein, dass $Q_{J,I}$ und $Q_{J',I'}$ die gleiche Quadrik darstellen, ohne dass $I = I'$ und $J = J'$ ist. Über diese Situation gibt der nächste Satz Auskunft. Um ihn zu formulieren, benötigen wir noch die folgende Bezeichnung. Sind X und Y Mengen, so bezeichne $X \triangle Y$ ihre symmetrische Differenz, das heißt die Menge

$$(X \cup Y) - (X \cap Y).$$

[5] Anmerkung der Herausgeber: der Autor hat hier einen Hinweis auf Fehler bei Bertini, Krull und Lense notiert.

Die Potenzmenge einer Menge versehen mit der symmetrischen Differenz als Verknüpfung ist bekanntlich eine elementarabelsche 2-Gruppe.

7.7. Satz. *Es sei V ein Vektorraum des Ranges n über dem kommutativen Körper K. Ferner seien I und I' zwei $(n-r-1)$- und J und J' zwei $(r-1)$-Teilmengen von $\{1,\dots,n\}$ mit $I \cap J \neq \emptyset \neq J' \cap I'$. Genau dann gibt es ein $k \in K^*$ mit $Q_{J,I} = kQ_{J',I'}$, wenn $I = I'$ und $J = J'$ oder wenn $I \triangle I' = J \triangle J'$ und $|I \triangle I'| = 2$ ist.*

Beweis. Es seien I und J Teilmengen von $\{1,\dots,n\}$ mit $|J| = r-1$, $|I| = n-r-1$ und $I \cap J \neq \emptyset$. Nach 7.3 ist bis auf ein Vorzeichen, das für unsere Untersuchungen irrelevant ist,

$$Q_{J,I}(z) = \sum_{|M|=r,\, M\cap I=\emptyset,\, J\subseteq M\cup I} a_M a_{J\cup\{i_M\}} C_{J\cup\{i_M\},M}.$$

Dabei ist i_M das Element aus der Gleichung $M \cup I \cup \{i_M\} = \{1,\dots,n\}$.

Es seien I' und J' zwei weitere Mengen der gleichen Art und es gebe ein $k \in K^*$ mit $Q_{J,I} = kQ_{J',I'}$. Wähle ein M mit $|M| = r$, $M \cap I = \emptyset$ und $J \subseteq M \cup I$. Wir definieren z durch $a_M := 1$, $a_{J\cup\{i_M\}} := 1$ und $a_L := 0$ für alle von M und $J \cup \{i_M\}$ verschiedenen L. Dann ist

$$Q_{J,I}(z) = a_M a_{J\cup\{i_M\}} C_{J\cup\{i_M\},M} \neq 0.$$

Es folgt, dass auch $Q_{J',I'}(z) \neq \emptyset$ ist. Es gibt also ein P mit $|P| = r$, $P \cap I' = \emptyset$ und $J' \subseteq P \cup I'$, so dass

$$a_P a_{J'\cup\{i'_P\}} \neq 0$$

ist. Wegen $P \neq J' \cup \{i'_P\}$ gibt es nun zwei Fälle, nämlich den
Fall 1: Es ist $M = P$ und $J \cup \{i_M\} = J' \cup \{i'_M\}$
und den
Fall 2: Es ist $P = J \cup \{i_M\}$ und $M = J' \cup \{i'_P\}$.

Wir zeigen, dass genau dann $I = I'$ gilt, wenn $J = J'$ ist. Dazu sei zunächst $I = I'$. In Fall 1 ergibt sich $i_M = i'_M$ und wegen $i_M \notin J$ und $i_M = i'_M \notin J'$ und $J' \cup \{i'_M\} = J \cup \{i_M\}$ dann $J = J'$. In Fall 2 ergibt sich der Widerspruch

$$\emptyset = I \cap M = I' \cap (J' \cup \{i'_P\}) \supseteq I' \cap J' \neq \emptyset.$$

Ist umgekehrt $J = J'$, so folgt in Fall 1 aus $J \cup \{i_M\} = J' \cup \{i'_M\}$, dass $i_M = i'_M$ ist. Dies impliziert wiederum $I = I'$. In Fall 2 folgt zunächst aus $I' \cap P = \emptyset$, dass $I' \cap J = \emptyset$ ist. Damit erhalten wir den Widerspruch

$$\emptyset \neq I' \cap J' = I' \cap J = \emptyset.$$

Es sei also $I \neq I'$ und $J \neq J'$. Wegen $|I| = |I'|$ ist dann

$$|I - I'| = |I' - I| \neq 0.$$

Es ist

$$|I^c \cap J| = |J| - |I \cap J| = r - 1 - |I \cap J| \leq r - 2.$$

Es sei $x \in I' - I$. Dann ist folglich

$$\big|(J - I) \cup \{x\}\big| \leq r - 1.$$

Es gibt also ein M mit $|M| = r$, $I \cap M = \emptyset$ und $(J - I) \cup \{x\} \subseteq M$. Mit diesem M liegt wegen $M \cap I' \neq \emptyset$ Fall 2 vor. Es ist also

$$M = J' \cup \{i'_P\}$$

und

$$P = J \cup \{i_M\}.$$

Wegen $x \in I'$ ist $x \neq i'_P$, so dass wegen $x \in M$ dann $x \in J'$ gilt. Weil x irgendein Element aus $I' - I$ ist, folgt $I' - I \subseteq J' \cap I'$. Wegen $\emptyset = I \cap M$ und $J' \subseteq M$ folgt $I \cap J' = \emptyset$. Daher ist

$$I' - I = J' \cap I'.$$

entsprechend folgt

$$I' \cap J = \emptyset$$

und

$$I - I' = J \cap I.$$

Setze $s := |I' - I|$. Dann ist auch $s = |I - I'|$. Es folgt

$$|I \cup (J \cap I^c) \cup (I' - I)| = n - r - 1 + r - 1 - s + s = n - 2.$$

Wäre nun $s > 1$, so gäbe es also ein M mit $|M| = r$, $M \cap I = \emptyset$, $J \cap I^c \subseteq M$ und $|M \cap I'| = s - 1$, so dass auch $M \cap I' \neq \emptyset$ wäre. Dann wäre aber $J' \subseteq M$ im Widerspruch zur Wahl von M. Dieser Widerspruch zeigt, dass doch $s = 1$ ist.

Es ist

$$|I \cup I'| = |I \cup (I' - I)| = n - r - 1 + 1 = n - r.$$

Wählt man nun $M := (I \cup I')^c$, so ist man in Fall 1 und es gilt

$$J \cup \{i_M\} = J' \cup \{i'_M\}.$$

Es folgt

$$J = (J \cap J') \cup \{i'_M\}$$

und

$$J' = (J \cap J') \cup \{i_M\}.$$

Es ist

$$i'_M \in (I' \cup M)^c = (I' \cup (I \cup I')^c)^c = I'^c \cap (I \cup I') = I'^c \cap I.$$

Also ist

$$I = (I \cap I') \cup \{i'_M\}.$$

Ebenso folgt
$$I' = (I \cap I') \cup \{i_M\}.$$
Damit ist gezeigt, dass
$$I \triangle I' = \{i'_M, i_M\} = J \triangle J'$$
ist. Damit ist die Notwendigkeit der Bedingungen des Satzes gezeigt.

Die Bedingungen des Satzes seien erfüllt. Ist $I = I'$ und $J = J'$, so ist $Q_{I,J} = Q_{J',I'}$. Es sei also $I \triangle I' = J \triangle J'$ und $|I \triangle I'| = 2$. Auf Grund von Satz 7.2 dürfen wir annehmen, dass folgendes gilt:
$$\begin{aligned} I \cap I' &= \{1, \ldots, n-r-2\} \\ I &= (I \cap I') \cup \{n-r-1\} \\ I' &= (I \cap I') \cup \{n-r\} \\ J \cap J' &= \{n-r+1, \ldots, n-2\} \\ J &= \{n-r-1\} \cup (J \cap J') \\ J' &= \{n-r\} \cup (J \cap J'). \end{aligned}$$
Für M, i_M und P gibt es wegen $I \cap M = \emptyset$ und $J \cap J' \subseteq M$ nur die folgenden drei Möglichkeiten:
$$\begin{aligned} M_1 &= (J \cap J') \cup \{n-1, n\} \\ M_2 &= (J \cap J') \cup \{n-r, n\} \\ M_3 &= (J \cap J') \cup \{n-r, n-1\} \end{aligned}$$
Es folgt $i_{M_1} = n-r$, $i_{M_2} = n-1$ und $i_{M_3} = n$. Für die zugehörigen P erhalten wir
$$\begin{aligned} P_1 &= (J \cap J') \cup \{n-1, n\} = M_1 \\ P_2 &= J \cup \{n-1\} \\ P_3 &= J \cup \{n\}. \end{aligned}$$
Es folgt $i'_{P_1} = n-r-1$, $i'_{P_2} = n$ und $i'_{P_3} = n-1$. Es sind nun die Koeffizienten $C_{J\cup\{i_M\},M}$ und $C'_{J'\cup\{i_P\},P}$ auszurechnen, wobei die Koeffizienten von $Q_{J',I'}$ mittels I' zu berechnen sind. Zur Erinnerung, es ist
$$C_{J\cup\{i_M\},M} = \prod_{\alpha\in M, \beta\in I} \langle \alpha, \beta \rangle \prod_{\gamma \in (J\cup\{i_M\})^c} \langle \gamma, i_M \rangle.$$
Mit $M := M_1$ und $P := P_1$ ergibt sich
$$C_{J\cup\{i_M\},M} = (-1)^{r(n-r-1)}(-1)^2 = (-1)^{rn}$$
und
$$C'_{J'\cup\{i'_P\},P} = (-1)^{r(n-r-1)}(-1)^2 = (-1)^{rn}.$$
Mit $M := M_2$ und $P := P_2$ ergibt sich
$$C_{J\cup\{i_M\},M} = (-1)^{r(n-r-1)}(-1) = (-1)^{rn-1}$$

und

$$C'_{J' \cup \{i'_P\},P} = (-1)^{r(n-r-1)-1} = (-1)^{rn-1}.$$

Mit $M := M_3$ und $P := P_3$ ergibt sich

$$C_{J \cup \{i_M\},M} = (-1)^{r(n-r-1)} = (-1)^{rn}$$

und

$$C'_{J' \cup \{i'_P\},P} = (-1)^{r(n-r-1)-1}(-1) = (-1)^{rn}.$$

Es ist also in der Tat

$$Q_{J,I} = kQ_{J',I'},$$

wobei

$$k = \epsilon_J \epsilon'_J \epsilon'_{J'} \epsilon''_{J'}$$

ist. Damit ist der Satz bewiesen.

Beim Beweise dieses Satzes wurde wieder wesentlich von der Kommutativität von K Gebrauch gemacht.

Gleiche Quadriken zu definieren, ist natürlich eine Äquivalenzrelation auf der Menge der $Q_{J,I}$. Ist $r = 2$, so ist es relativ einfach, die Anzahl der Äquivalenzklassen abzuzählen. Dies liegt daran, dass in diesem Falle $J \subseteq I$ und $|J| = 1$ gilt.

7.8. Satz. *Es sei V ein Vektorraum des Ranges $n \geq 4$ über dem kommutativen Körper K. Dann ist $G_2(V)$ Schnitt von*

$$\sum_{i:=0}^{n-4} \binom{i+2}{i} (n-3-i)$$

Quadriken von $\mathrm{L}(\bigwedge_K^2(V))$.

Beweis. Es sei I eine $(n-3)$-Teilmenge von $\{1, \ldots, n\}$ und es sei $J = \{k\}$ mit $k \in I$. Ist $1 \notin I$, so setzen wir $I' := I \triangle \{1, k\}$ und $J' := I \triangle \{1, k\}$. Dann ist $J' = \{1\}$ und $|I'| = n - 3$ sowie $1 \in I'$. Mit Satz 7.7 folgt, dass $Q_{J,I}$ und $Q_{J',I'}$ die gleiche Quadrik darstellen. Daher dürfen wir im Folgenden stets annehmen, dass $1 \in I$ gilt.

Mit Z_j bezeichnen wir die Menge der ersten j natürlichen Zahlen. Ferner setzen wir

$$\Pi_i := \{I \mid |I| = n-3, Z_{n-3-i} \subseteq I, n-2-i \notin I\}$$

für $i := 0, \ldots, n-4$.

Es ist $\Pi_0 = \{Z_{n-3}\}$. Daher liefern die I aus Π_0 — es gibt nur eines — genau $n-3$ quadratische Formen $Q_{J,I}$. Es sei bereits bewiesen, dass die $I \in \bigcup_{j:=0}^{i} \Pi_j$ genau $\sum_{j:=0}^{i} \binom{j+2}{j}(n-3-j)$ verschiedene quadratische Formen liefern.

Es sei $I \in \Pi_{i+1}$. Ferner sei $x \in I$. Setze $Z := Z_{n-3-(i+1)}$. Ist $x \notin Z$, so folgt

$$|I - (Z \cup \{x\})| = n - 3 - (n-3-i-1) - 1 = i.$$

Setze $L := I - (Z \cup \{x\}$ und $I' := Z_{n-3-i} \cup L$, so ist $I' \in \Pi_i$ und es folgt mit 7.7, dass $Q_{\{x\},I}$ und $Q_{\{n-4-i\},I'}$ die gleiche Quadrik darstellen. Wir erhalten also höchstens dann eine neue quadratische Form, wenn $x \in Z$ ist. Ist $x \in Z$, so kommt $Q_{\{x\},I}$ unter den bereits konstruierten Formen wegen 7.7 auch nicht vor. Schließlich folgt, dass die neu konstruierten Formen auch alle untereinander verschieden sind. Wegen $Z = Z_{n-3-i-1} \subseteq I$ und $n - 2 - i - 1 \notin I$ gibt es für $I - Z$ dann noch

$$\binom{i+3}{i+1}$$

Möglichkeiten. Damit liefern die $I \in \Pi_{i+1}$ weitere

$$\binom{i+1+2}{i+1}(n-3-(i+1))$$

Formen. Damit ist der Satz bewiesen.

Für $n = 4$ erhalten wir, wie schon zuvor, dass $G_2(V)$ eine Quadrik ist. Für $n = 5, 6, 7, 8, 9$ ist $G_2(V)$ Schnitt von 5, 15, 35, 70, 126 Quadriken in $\mathrm{L}(\bigwedge_K^2(V))$.

Anhang

Der Aufbruch der Geometrie um Reinhold Baer in Frankfurt und seine Protagonisten — in memoriam Heinz Lüneburg

Vortrag von Karl Strambach beim Baer–Kolloquium
in Kaiserslautern am 7. November 2009

Liebe Frau Lüneburg, lieber Martin, liebe Freunde !

Als ich verspätet, durch persönliche Umstände bedingt, in Mai 1961 begann, in Frankfurt Physik zu studieren, haben mich, obgleich von der Mathematik vollkommen unbeleckt, die Mathematikvorlesungen am meisten angezogen. Es eröffnete sich mir eine neue faszinierende Welt, die ich näher kennenlernen wollte, obgleich ich mir meines Unvermögens halbwegs bewusst war. Es war ein Glücksfall, dass ich Annemarie Schlette traf, die mir begeistert vom Baerschen Laden erzählte, wo man von allen Zwängen frei Mathematik lernen könne, und mir half, bei Helmut Salzmann einen Proseminarvortrag zu ergattern. So kam ich 1962 ins Baersche Wunderland, in dem neue Sätze wie Pilze aus dem Boden sprossen. Ich war fast geblendet von der Vielzahl der Talente, die um mich umherschwirrten und fast wöchentlich Neues zu berichten hatten. Auch die Spannweite der erzielten Resultate war immens: In der Algebra waren es etwa gruppentheoretische Eigenschaften, Engelsche Elemente, Faktorisierung von Gruppen, distributive Quasigruppen, Erweiterungen abelscher Gruppen und ringtheoretische Radikale, in der Geometrie waren es endliche und topologische Ebenen, Möbius- und Laguerregeometrie und gruppentheoretische Methoden in der Geometrie, die die Gemüter erhitzten.

Ich fühlte mich in diesem mathematischen Karpfenteich zur Geometrie hingezogen, weil ich mir einbildete, die Geometrie ist etwas Handfestes, Greifbares und bei meinen geringen mathematischen Kenntnissen eher Zugänglicheres. Dass ich heute vor Ihnen stehen darf, ist nicht mein Verdienst, sondern das von Helmut Salzmann, der mich behutsam an die Hand nahm und mir nicht nur die Geometrie, ja die Mathematik erschloss.

Dass die Geometrie in Frankfurt in der Zeit des Baerschen Wirkens sich zu prachtvoller Blüte entfalten konnte, war der faszinierenden, einnehmenden, junge Mathematiker begeisternden und sie ermutigenden Persönlichkeit von Reinhold Baer zu verdanken, der von 1940 bis 1952 selbst grundlegende Arbeiten über endliche projektive Ebenen, man denke etwa an den von daher stammenden Begriff einer Baer-Unterebene, und ein Buch „Linear Algebra and Projective Geometry" verfasst hat. Die Geometrie lag Reinhold Baer lebenslang am Herzen; davon zeugt auch diese Tagungsreihe, die er zusammen mit Herrn Pickert begründet hat und die auch heute seinen Namen trägt. Ein weiterer glücklicher Umstand für die Geometrie war Ruth Moufang, die Kollegin von Reinhold Baer war und ihre Schüler ebenfalls für die Grundlagen der Geometrie und konvexe Körper einzunehmen wusste. Die Symbiose zwischen dem Baerschen und Moufangschen Kreis war so perfekt, dass für mich Peter Dembowski ein fester Bestandteil der Baerschen Geometriegruppe war, obgleich sein Talent wohl von Frau Moufang entdeckt worden war.

Die Baersche Geometriegruppe, die sich der endlichen Geometrie, ihren kombinatorischen Aspekten sowie ihren Verbindungen zur Gruppentheorie verschrieben hatte, hatte nach meiner damaligen Überzeugung, und daran hat sich bis heute nichts geändert, drei tragende Säulen: Peter Dembowski, Heinz Lüneburg und Christoph Hering. Obgleich die zeitlichen Unterschiede beim Einstieg in mathematische Publikationstätigkeit dieser drei Pilaster aus heutiger Sicht vernachlässigbar erscheinen, die erste Arbeit von Peter Dembowski erschien 1958, die von Heinz Lüneburg 1960 und die von Christoph Hering 1963, für mich als Studenten und Bewunderer gehörten sie drei verschiedenen Generationen an.

Peter Dembowski war für mich der abgeklärte Wissenschaftler, der aus dem Nichts, d.h. ohne kompliziertere Theorien benutzend, bleibende markante Resultate hervorzaubern konnte. Als hervorstechendstes Beispiel sei hier an seine Habilitationsschrift über Möbiusebenen gerader Ordnung erinnert, in der bewiesen wird, dass jede endliche Möbiusebene, in der jeder Kreis eine ungerade Anzahl von Punkten trägt, ovoidal ist; dies geschieht dadurch, dass er durch raffinierte Abzählkünste den dreidimensionalen Raum mit Hilfe der Winternitzschen Axiome erschafft und die Möbiusebene als ein Ovoid hineinlegt. Durch diese Arbeit hat insbesondere die Klassifikation von Ovoiden in projektiven Räumen über Galoisfeldern gerader Charakteristik an Bedeutung gewonnen und dazu geführt, dass man heutzutage intensiv sogar den Computer einsetzt, um außer den elliptischen und den Tits–Ovoiden neue Ovoide zu entdecken. Bis jetzt ist man zu projektiven Räumen über Galoisfeldern der Ordnung 2^n mit $n \leq 5$ vorgedrungen, hat aber nach meiner Kenntnis leider keine neuen Ovoide gefunden. Peter Dembowski war und ist für mich derjenige der drei Frankfurter Sterne der diskreten Geometrie, der es liebte, endliche Geometrien in einen kombinatorischen Kontext zu rücken.

Christoph Hering empfand ich als ein jugendliches Nachwuchsgenie, der Tolles leistet und durch seinen augenzwinkernden Humor es verhindert, als Zelebrität wahrgenommen zu werden. Unvergessen bleiben mir seine Vorträge über die Lenz–Barlotti–Klassifikation von Möbiusebenen, heutzutage Hering Klassi-

fikation genannt, bei den Kindertagungen in Oberwolfach. Obgleich er bis Mitte der achtziger Jahre im Geiste der Frankfurter endlichen Geometrie gearbeitet und publiziert hat, empfinde ich ihn als einen Geometer, der den endlichen Gruppen, gesehen als Automorphismengruppen, sein unbedingtes Interesse und seine Phantasie geschenkt hat.

Heinz Lüneburg altersmäßig zwischen den beiden, Dembowski und Hering, stehend war für mich die Achse der Frankfurter Forschung über nichttopologische Geometrie. In seinen Arbeiten über endliche Geometrie bewegte er sich äquidistant zwischen Kombinatorik und Gruppentheorie und klopfte außerdem die damaligen Strömungen der geometrischen Forschung auf ihre Entwicklungsfähigkeit ab. Davon zeugen seine Arbeiten über λ–Räume, Hjelmslev–Ebenen, Blockpläne, insbesondere Steinersche Tripel- und Quadrupelsysteme, Fundamentalsätze der projektiven Geometrie, die Rolle der Zentral- und Axialkollineationen sowie über elliptische Ebenen.

Die erste große Leidenschaft von Heinz Lüneburg, der 1956 sein Studium in Frankfurt begann, also in dem Jahr, in dem Reinhold Baer aus Amerika zurückkehrend einen Lehrstuhl in Frankfurt akzeptierte, galt der kleinen Reidemeisterbedingung. Die Reidemeisterbedingung ist ein Schließungssatz, der in der Theorie der Loops und der zugehörigen Netze die Assoziativität garantiert und am bequemsten mit Hilfe von Projektivitäten in 3-Netzen formulierbar ist. Eine Spezialisierung dieses Schließungssatzes war für Andrew Gleason der Angelpunkt beim Beweis des Satzes, dass eine endliche Fano–Ebene, d.h. eine endliche Ebene, in der die Diagonalpunkte eines jeden Vierecks kollinear sind, pappossch sein muss. Dass man, um dieses Resultat zu erreichen, die Kollinearität der Diagonalpunkte eines jeden Vierecks wirklich verlangen muss, sieht man bereits in der projektiven Ebene über einem Fastkörper der Ordnung 9, denn in dieser existieren gewisse Vierecke mit kollinearen Diagonalpunkten. Die Gleasonsche Arbeit muss im Baerschen Seminar heftig studiert worden sein und Heinz Lüneburg zu der Vermutung geführt haben, dass jede endliche projektive Ebene, in der die kleine Reidemeisterbedingung gilt, bereits desarguessch sein muss. Er hat diese Vermutung in drei Arbeiten eindrucksvoll bestätigt, wobei er in der zweiten Arbeit sein Ziel bis auf eine Ausnahme, nämlich die der Ebenen der Ordnung 60 erreicht hat. Die Schlachtung dieser Ebenen gelang ihm zusammen mit Otto Kegel, dem Meister der Faktorisierung, mit Hilfe des folgenden Satzes: Ist $G = A \cdot B$ Produkt zweier echter Untergruppen A und B und sind sowohl A als auch B isomorph zur alternierenden Gruppe des Grades 5, so ist G entweder das direkte Produkt $A \times B$ oder die alternierende Gruppe des Grades 6. Diese gemeinsame Arbeit von Heinz Lüneburg mit Otto Kegel gibt ein beredtes Zeugnis davon, dass die an verschiedenen Beeten des Baerschen Forschungsgartens Tätigen miteinander in enger Kommunikation standen und einander unterstützten.

Innerhalb der Gruppentheorie sind es die Suzuki–Gruppen, die sich zu Lieblingsobjekten von Heinz Lüneburg entwickelten und ihn jahrelang treu begleiteten. Ausgangspunkt für diese Zuneigung waren die von Dembowski gepflegten endlichen Möbiusebenen. Heinz Lüneburg beweist 1964, dass eine endliche Möbiusebene M, deren Automorphismengruppe auf den Punkten von M zwei-

fach transitiv ist, wobei aber nur die Identität drei verschiedene Fixpunkte hat, entweder miquelsch oder die Geometrie der ebenen Schnitte eines Tits–Ovoids ist. Später zeigt er, dass sich die gleiche Folgerung ergibt auch für kreishomogene endliche Möbiusebenen oder für endliche Möbiusebenen gerader Ordnung, die eine transitive Automorphismengruppe gerader Ordnung gestatten. Da die Automorphismengruppen von Tits–Ovoiden Suzuki–Gruppen sind, ist die Begegnung von Heinz Lüneburg mit diesen Gruppen unumgänglich. Und nachdem er sich mit ihnen eingehender befasst hat, sieht er, dass sie für ihn eine Brücke zu den Translationsebenen schlagen, indem er den folgenden Satz beweist: Ist $q = 2^{2r+1} \geq 8$, so gibt es genau eine Translationsebene, die die Ordnung q^2 hat und eine zur Suzuki–Gruppe der Ordnung $(q^2 + 1)q^2(q - 1)$ isomorphe Kollineationsgruppe besitzt; diese Ebene ist nicht desarguessch.

Die Translationsebenen waren in Frankfurt wohlbekannt, denn T. G. Ostrom, dessen Lecture notes „Finite translation planes“ die erste zusammenfassende Darstellung diese Gebietes war, besuchte häufig den Baerschen Kreis in Frankfurt und seine Vorträge über replaceable nets klingen mir noch heute in den Ohren. So war Heinz Lüneburg bestens über den Forschungsstand bezüglich endlicher Translationsebenen informiert und konnte diese Ebenen, die seinen Namen tragen, in einer großen Arbeit für die Hamburger Abhandlungen in einen größeren Rahmen der endlichen projektiven Ebenen einbetten, deren von den Elationen erzeugte Kollineationsgruppe Punktstabilisatoren vorgeschriebener Struktur hat. Eine schöne Charakterisierung der Lüneburgebenen hat 1972 Liebler gegeben: Die Lüneburgebenen sind diejenigen affinen Translationsebenen, bei denen eine Gruppe G von Kollineationen als Gruppe vom Rang drei auf der Menge der eigentlichen Punkte (d.h. der Stabilisator jedes eigentlichen Punktes in G hat drei Bahnen) und als Gruppe vom Rang zwei auf der Menge der uneigentlichen Punkte operiert.

Den Kulminationspunkt Lüneburgscher Forschungen über endliche Translationsebenen stellt seine 1980 erschienene Monographie „Translation planes“ dar. Nachdem er in ihr die nötigen Grundlagen zusammengestellt hatte, diskutiert er permutationstheoretische Kriterien, die es sicherstellen, dass eine endliche projektive oder affine Ebene, auf der eine Gruppe G von Kollineationen operiert, eine Translationsebene ist und G die Translationsgruppe enthält. Von den dort behandelten Kriterien von Ascher Wagner, Kallaher, Ostrom sei eine Charakterisierung von Heinz Lüneburg, die für seine Ebenen zutrifft, besonders erwähnt: Ist A eine endliche affine Ebene und G eine Gruppe von Kollineationen von A, so dass der Stabilisator jeder Geraden von A in G auf den Punkten dieser Geraden zweifach transitiv ist, so ist A eine Translationsebene und G enthält die Translationsgruppe.

Der Löwenanteil der Lüneburgschen Monographie ist jedoch speziellen, signifikanten Translationsebenen gewidmet, die in keinen großen Familien leben, sondern eher ein Einsiedlerdasein führen. Von den von Heinz Lüneburg entdeckten und zuerst in Geometriae Dedicata publizierten Translationsebenen, die er merkwürdige Translationsebenen nennt, gibt es zwei Typen, die sich in der Struktur gewisser Elationsgruppen unterscheiden; von dem einem Typ gibt es 8 nichtisomorphe, von dem andern Typ gibt es 14 nichtisomorphe Ebenen. Auch

im Kapitel VII, welches der Klassifikation von Translationsebenen der Ordnung q^2 gewidmet ist, die den Körper $\mathrm{GF}(q)$ in ihrem Kern enthalten und eine zu $\mathrm{SL}_2(q)$ isomorphe Kollineationsgruppe gestatten, ist das Hauptaugenmerk auf die Hering– und Schäffer–Ebenen gerichtet.

Dass sich Heinz Lüneburg in den achtziger Jahren den endlichen Translationsebenen entfremdet hat, kann man verstehen, wenn man in das neueste, 2007 erschienene und 888 Seiten umfassende „Handbook of finite translation planes“ von Norman Johnson, Vikram Jha und Mauro Biliotti hineinschaut, in dem alle bisher bekannten endlichen Translationsebenen gesammelt sind. Um in diesem Karpfenteich auch heutzutage noch erfolgreich zu fischen, braucht man nicht nur Ausdauer und Geduld, sondern auch eine Buchhalterveranlagung, die Heinz Lüneburg wohl abging.

Neben den Suzuki–Gruppen galt Lüneburgs Interesse auch anderen extravaganten endlichen Gruppen, so etwa den Ree–Gruppen und den Mathieu–Gruppen sowie deren Darstellungen als Automorphismengruppen geeigneter Blockpläne.

Lüneburgsche Arbeiten, in denen keine abschließenden Antworten der behandelten Probleme gegeben wurden, enthielten stets eine Fülle von Anregungen und Methoden, die die Leser dieser Arbeiten zum Weiterforschen anregten. So haben seine Arbeiten zur Existenz der endlichen projektiven Ebenen vom Lenz–Barlotti–Typ I.6 und III.2 Hering und Kantor inspiriert zu beweisen, dass es weder eine endliche projektive Ebene vom Lenz–Barlotti–Typ I.6 noch eine Ebene vom Lenz–Typ III gibt. Ich glaube, dass bis heute ungeklärt ist, ob es unendliche projektive Ebenen vom Lenz–Barlotti–Typ I.6 gibt. Der einzige andere offene Fall scheinen die endlichen projektiven Ebenen vom Lenz–Barlotti–Typ II.1 zu sein. Meine Quelle für diese Behauptungen ist: Gina Ghinelli and Francesca Merola, Lenz–Barlotti–Classification and related open problems: an update, Roma 2005, Quaderni Elettronici del Seminario di Geometria Combinatoria (Quaderno 20).

Obgleich ich mich nie direkt im unmittelbaren Umkreis Lüneburgscher Forschungen aufgehalten habe, gibt es zwei Themen, wo sich unsere Interessen berührt haben. Einmal ist es die Funktionalgleichung $f(x + yf(x)) = f(x)f(y)$ von Golab und Schinzel, die die Beziehungen zwischen Komplementen eines semidirekten Produkts regelt. Peter Plaumann und ich haben diese Funktionalgleichung über den p-adischen Zahlen traktiert, Heinz Lüneburg und Peter Plaumann haben sie über den Galoisfeldern behandelt. Das zweite Thema, das Heinz Lüneburg und mich faszinierte, sind die Gruppen der Projektivitäten eines Blocks auf sich in verschiedenen Geometrien, also der von Staudtsche Standpunkt.

Nachdem Carl Georg Christian von Staudt Mitte des neunzehnten Jahrhunderts die Gruppe Π der Projektivitäten einer Geraden auf sich in einer papposschen projektiven Ebene E betrachtet und bewiesen hatte, dass sie scharf dreifach transitiv ist, und nachdem mit Hessenberg klar war, dass E genau dann papposch ist, wenn Π scharf dreifach transitiv und dann isomorph zu $\mathrm{PGL}(2, K)$ ist, hat die Schönheit dieses Satzes die Geometer so eingelullt, dass die naheliegende Frage, wie es um die Gruppe Π der Projektivitäten einer Gera-

den auf sich in anderen, insbesondere nichtdesarguesschen projektiven Ebenen steht, lange nicht gestellt wurde. Erst 1959 hat sich Adriano Barlotti diesem Problem gestellt und bewiesen, dass die Gruppe Π der Projektivitäten in den drei nichtdesarguesschen Ebenen der Ordnung 9 die symmetrische Gruppe des Grades 10 und in der Hallebene der Ordnung 16 die alternierende Gruppe des Grades 17 ist. Damit war die Hatz auf die Gruppe Π der Projektivitäten in nichtdesarguesschen endlichen Ebenen eröffnet. Nachdem sie in vielen endlichen projektiven Ebenen bestimmt worden war, hatte sich schnell die Vermutung herauskristallisiert, dass die Gruppe Π der Projektivitäten in endlichen nichtdesarguesschen projektiven Ebenen der Ordnung n stets die alternierende Gruppe des Grades $n+1$ enthalten muss. Da jedoch in den sechziger Jahren die Klassifikation der endlichen einfachen Gruppen noch ausstand, trotzte diese Vermutung jedem Angriff.

Obgleich Heinz Lüneburg in den Beweisen seiner Arbeiten ausgiebig Projektivitäten zwischen Geraden benutzt hatte, trat er mit der Gruppe der Projektivitäten an die Öffentlichkeit erst mit seiner 1967 veröffentlichten Arbeit, in der die desarguesschen affinen Ebenen als diejenigen affinen Ebenen gekennzeichnet werden, in denen es zu je drei verschiedenen Punkten P, Q, R ein (axiomatisch definiertes) Teilverhältnis r gibt, so dass $PrQ = R$ gilt. Der Satz, in dem die Gruppe der Projektivitäten dabei mit voller Wucht auftritt, ist das folgende Nebenergebnis der Arbeit: Eine endliche projektive Ebene ungerader Ordnung q ist genau dann desarguessch, wenn der Stabilisator eines Punktes in der Gruppe der Projektivitäten einer Geraden auf sich einen Normalteiler der Ordnung q enthält. Außerdem wird einem bei der Durchsicht dieser Arbeit klar, dass der Verfasser wusste, man müsse mit gleichem Nachdruck wie die Gruppe Π der Projektivitäten einer projektiven Ebene in affinen Ebenen auch die Gruppe der affinen Projektivitäten einer affinen Geraden auf sich studieren, deren Elemente Produkte affiner Parallelperspektivitäten sind.

Die Beschäftigung von Heinz Lüneburg mit den Gruppen von Projektivitäten erreicht ihren Höhepunkt in dem Bericht „Some new results on groups of projectivities“, welcher die Frucht seiner Vorträge bei der Bad Windsheimer Tagung „Geometry – von Staudt's Point of View“ ist. In diesem Beitrag wird auch über die Ergebnisse seines Schülers Theo Grundhöfer, insbesondere bezüglich der Gruppe der affinen Projektivitäten, ausführlich berichtet.

Da inzwischen eine Klassifikation der endlichen einfachen Gruppen vorgelegen hatte, war Theo Grundhöfer in der Lage, die Vermutung über die Gruppen Π der Projektivitäten in endlichen nichtdesarguesschen projektiven Ebenen fast vollständig zu beweisen: Die Gruppe Π der Projektivitäten einer endlichen nichtdesarguesschen projektiven Ebene der Ordnung n enthält entweder die alternierende Gruppe des Grades $n+1$ oder es ist $n = 23$ und Π ist die größte Mathieugruppe M_{24}. Dass die zweite Möglichkeit ausgeschlossen ist, haben neuerdings Peter Müller und Gabor Nagy gezeigt. Eine analoge Situation liegt nach Theo Grundhöfer, Peter Müller und Gabor Nagy auch für die Gruppe Σ der affinen Projektivitäten einer Geraden auf sich in einer affinen Ebene der Ordnung n vor, welche keine Translationsebene ist: Σ enthält entweder die alternierende Gruppe der Ordnung n oder, was natürlich unwahrscheinlich ist, es

ist $n = 24$ und die Gruppe Σ ist die Mathieu–Gruppe des Grades 24. Für Translationsebenen der Ordnung q^d mit dem Kern $\mathrm{GF}(q)$ hat bereits in den achtziger Jahren Theo Grundhöfer bewiesen, dass die Gruppe der affinen Projektivitäten eine Gruppe von affinen Abbildungen ist, so dass der Stabilisator eines Punktes zwischen $\mathrm{SL}(d, q)$ und $\mathrm{GL}(d, q)$ liegt.

Heinz Lüneburg war für mich ein leidenschaftlicher Mathematiker, dessen Vorträge und Vorlesungen so sorgfältig vorbereitet waren, dass sie sofort zum Druck gehen konnten. Auf diese Weise sind die folgenden seiner Bücher entstanden: „Kombinatorik“, erschienen 1971, „Einführung in die Algebra“, erschienen 1973, „Vorlesungen über Zahlentheorie“, erschienen 1978, „Galoisfelder, Kreisteilungskörper und Schieberegisterfolgen“, erschienen 1979, „Vorlesungen über Analysis“, erschienen 1981, „On the rational normal form of endomorphisms. A primer to constructive algebra“ und „Kleine Fibel der Arithmetik“, beide erschienen 1987, „Tools and fundamental constructions of combinatorial mathematics“, erschienen 1989, „Vorlesungen über lineare Algebra. Versehen mit der zu ihrem Verständnis nötigen Algebra sowie einigen Bemerkungen zu ihrer Didaktik“, erschienen 1993, „Die euklidische Ebene und ihre Verwandten“ und „Gruppen, Ringe, Körper. Die grundlegenden Strukturen der Algebra“, beide erschienen 1999 sowie „Rekursive Funktionen“, erschienen 2002. Diese für die Studierenden bestimmten Werke wollen keine Enzyklopädien über die in ihnen behandelten Gebiete sein, sondern spiegeln die persönliche Sicht des Verfassers wider, welche Sachverhalte man mehr gewichten soll und was vernachlässigbar ist, weil es in anderen Büchern schon hundertmal gesagt worden ist. In ihnen erweist sich Heinz Lüneburg als ein begnadeter Didaktiker, der nicht durch Beiwerk, sondern durch die Klarheit des Gedankens und durch strenge Beweisführung überzeugt. Dies konnte man übrigens bei jedem seiner Vorträge bewundern. Obwohl voll innerer Begeisterung und in der Überzeugung Wertvolles beizutragen, stand sein schnörkelloser direkter Vortragsstil im Gegensatz zu dem derjenigen Mathematiker, die in ihren Vorträgen an einer Wagneroper stricken.

Heinz Lüneburg war für mich ein Freund, der seinen Prinzipien ein Leben lang treu blieb und dessen erfolgreiche Karriere ihn weder verbogen noch vom täglichen Leben separiert hat. Wenn er einmal nach reifer Überlegung zu einem Urteil gekommen ist, war er davon durch Opportunitätsgründe nicht abzubringen. Dies hat ihm, dem Bildungswertkonservativen, in den Fakultätssitzungen, in denen häufig nach Anpassung an Umbrüche verlangende politische Vorlagen gehechelt wird, sicherlich nicht nur Beifall beschert.

Heinz Lüneburg hatte ein sensibles Ohr für Veränderungen in der Mathematik. Er suchte nach zeitloser Mathematik, nahm jedoch wahr, dass seit den achtziger Jahren durch den steigenden Publikationszwang bei den Mathematikern die Lust abnahm, einzelne Texte zu studieren, und wie im Sport der Wettbewerbscharakter in den Vordergrund rückte. Heutzutage zählt nicht nur der Gehalt einer mathematischen Arbeit, sondern auch im großen Maße in welch aggressivem Umfeld sie entstanden ist und ob sie ein Problem löst, an welchem sich schon einige mehr oder minder prominente Mathematiker die Zähne ausgebissen haben. Der Kampf der Teilgebiete der Mathematik um die Oberhoheit

in Zeitschriften mit hohem impact factor, der eine scheinbare Objektivierung mathematischer Leistung erlauben soll, ist voll entbrannt.

Heinz Lüneburg war gegenüber den modernen Entwicklungen der Mathematik aufgeschlossen, wollte aber nicht in Abstraktionen der Schemata, Moduli und Motive einsteigen, deren Wolkenhaftigkeit man überwinden muss, wenn man sich bei ihnen wohlfühlen will. Als Geometer ist man letztlich Greifbares gewohnt. Darüber hinaus hat ihn die Entwicklung elektronischer Rechenanlagen fasziniert und so hat er sich den Algorithmen zugewandt, mit denen man effektiv elementare zahlentheoretische Funktionen berechnen kann, wie etwa den größten gemeinsamen Teiler bzw. das kleinste gemeinsame Vielfache zweier ganzer Zahlen, die Einheiten im Ring der ganzen Zahlen modulo n, die Primitivwurzeln modulo einer Primzahl, oder die größte natürliche Zahl, die die Quadratwurzel einer gegebenen natürlichen Zahl nicht übertrifft. Er zeigte, wie man auch für inneralgebraische Fragestellungen, wie etwa die effektive Konstruktion der algebraischen Erweiterungen der Primkörper $\mathrm{GF}(p)$ sowie der vollständigen Kreisteilungskörper, Algorithmen einsetzen kann.

Heinz Lüneburg war der festen Überzeugung, dass der Computer ein Diener der Mathematiker bleiben muss (so etwa bei Schleifeninvarianten, von denen er behauptet, sie seien ihm fast zu einer fixen Idee geworden) und sich nicht als Herr etablieren darf. Da er wohl mit der Zeit merkte, dass diese Tendenz dem Zeitgeist immanent war, hat er sich, anstatt unnütze Scharmützel zu führen, aufgemacht, nach den Wurzeln der Mathematik zu suchen. Dafür war er bestens präpariert: Als Schüler des bekannten Frankfurter humanistischen Lessing–Gymnasiums, des Altgriechischen wie des Lateinischen mächtig, stand er fest und mit voller Überzeugung zu den Grundsätzen des Abendlandes. Nicht nur im Deutschen, sondern auch im Englischen, Französischen und Italienischen zu Hause, war er ein Verfechter einer abendländischen Idee, welche nicht nur aus der anglo-sächsischen Monokultur ihre Kraft bezieht.

Der großartige Einstieg von Heinz Lüneburg bei seiner Suche nach den geschichtlichen Wurzeln der Mathematik war das Ergebnis eines akribischen Studiums des Liber Abacci von Leonardo Pisano. In dem daraus entstandenen Buch „Leonardi Pisani Liber Abacci oder Lesevergnügen eines Mathematikers“, das zwei Auflagen erlebte, wird nicht nur eine Interpretation des Textes von Leonardo Pisano in der Sprache der uns geläufigen Mathematik gegeben, sondern auch ein Bild der Zeit ausgebreitet, in der Leonardo Pisano lebte und wirkte. Es ist keine kritische Edition, aber Heinz Lüneburg findet hier seine in allen späteren historischen Arbeiten angewandte Methode, den Lesern die Ergebnisse aus der Geschichte der Mathematik in modernem Gewand nahezubringen. So lässt er etwa Euler, Gauß und Lagrange von Körpern reden, obwohl das Konzept eines Körpers erst von Steinitz 1910 entwickelt wurde. Ebenso zeigt sich bereits hier, auch durch seine etymologischen Kenntnisse befördert, dass Heinz Lüneburg zum Urgrund der Mathematik, zur Zahl, zur Ziffer und und deren Herkunft vordringen will; natürlich spielt dabei die Null, ursprünglich as-sifr, latinisiert ciffra genannt, eine besondere Rolle.

Mir hat die Lektüre des ersten Kapitels von Lüneburgs Leonardi Pisani Liber Abacci neue überraschende Einsichten gebracht. Von der Geschichte

der Mathematik unbeleckt, war mir zwar klar, dass die Griechen, indem sie die Nabelschnur zwischen Wirklichkeit und insbesondere den Anwendungen durchgeschnitten hatten, die Geburtshelfer der Mathematik im heutigen Sinn sind. Doch von den Römern dachte ich, dass die Eroberung der Welt sie so in Anspruch nahm, dass keine Zeit zum mathematischen Spintisieren übrig blieb. Und von der katholischen Kirche des Mittelalters hatte ich den Eindruck der Gleichgültigkeit gegenüber der Mathematik. Meine Meinung war, dass die Mathematik nach den Griechen ihr Dasein in arabischem und jüdischem Umfeld, etwa in Spanien, gefristet hatte, ehe sie von der Renaissance wiedergeboren wurde. Heinz Lüneburg hat mich belehrt, dass diese naive Vorstellung falsch ist. Das römische Reich hatte ein gut ausgebautes Bildungssystem, in den Klöstern wurden griechische Schriften studiert und es gab hohe kirchliche Würdenträger, die sich um den Erhalt des naturwissenschaftlichen Wissens der Griechen sorgten. Und das Buch Liber Abacci selbst gibt Zeugnis davon, dass der Fluss der Mathematik in keiner Periode des Mittelalters ausgetrocknet ist.

Die zweite Überraschung, die mir Heinz Lüneburg mit seinem Buch bescherte, betrifft Palermo, wo ich jetzt jedes Jahr einige Zeit zubringe. Mir erschien die Eroberung von Palermo durch die Normannen im positiven Licht, wobei ich diese Ansicht aus der Solidität des Palazzo dei Normanni, der Schönheit der Capella Palatina und der imponierenden Pracht des Doms von Monreale bezog. Doch bei Heinz Lüneburg kann man nachlesen, dass die Pisaner, die die Normannen bei deren Kampf gegen die Sarazener unterstützten, Palermo nach dessen Eroberung so tüchtig plünderten, dass sie aus dem Erlös der Beute in Pisa den von den Touristen bestaunten Dom auf der Piazza dei miracoli erbauen konnten. Meine Meinung über Kaiser Friedrich den Zweiten, an dessen Grab ich in der Palermitaner Kathedrale ab und zu vorbeischlendre, hat Heinz Lüneburg vollauf bestätigt: Friedrich der Zweite war nicht nur ein ausgewiesener Experte der Falknerei, sondern auch ein entschiedener Förderer der Wissenschaften und Begründer der Universität Neapel.

Das letzte von Heinz Lüneburg erschienene Werk sind die beiden Bände betitelt „Von Zahlen und Größen. Dritthalbtausend Jahre Theorie und Praxis“, die der Geschichte der algebraischen Gleichungen und der Körper gewidmet sind. Sie sind, wie bei Lüneburg üblich, in der Sprache der heutigen Mathematik verfasst, enthalten aber unzählige historische und etymologische Ausflüge, natürlich auch in Latein und Italienisch, und einige Bemerkungen, die zeigen, dass der Autor der verlorenen klassischen Bildung der Jugend und der gerade jetzt vor unseren Augen sterbenden Humboldtschen Universität nachtrauert.

Heinz Lüneburg hat sich selbst nicht als Mathematikhistoriker betrachtet. Er sagt, dass er bei einem Gegenstand mehr in die Tiefe, während der Historiker mehr in die Breite geht. Ich möchte hier aus den Vorlesungen zur Geschichte der Mathematik von Hans Wussing, dem auch heute noch berühmten Mathematikhistoriker aus Leipzig, zitieren, um Ihnen die Entscheidung zu erleichtern, ob es unbedingt eine Ehre sein muss, zur professionellen Zunft der Wissenschaftshistoriker zu gehören. Wussing führt auf Seite 18 aus: Die marxistische Historiographie der Mathematik beruht methodologisch auf dem historischen und dialektischen Materialismus. Danach ist jede Wissenschaft eine gesellschaftliche Er-

scheinung. Auch die Mathematik ist eine spezifische Form des gesellschaftlichen Bewusstseins. Sie ist mehr als das Ergebnis von Kenntnissen und Erkenntnissen, von Theorien und Methoden; sie ist zugleich geformt von den materiellen und ideellen Interessen der jeweils herrschenden Klassen.

Heinz Lüneburg wurde jäh aus dem Leben gerissen, er war bis zum letzten Tag voller mathematischer Ideen und beabsichtigter Buchprojekte. Martin Lüneburg und Theo Grundhöfer fanden denn auch im Nachlass drei Werke, die es lohnten publiziert zu werden. Zwei von ihnen waren von Heinz Lüneburg so vollständig bearbeitet, dass sie, versehen mit marginalen Bemerkungen der Herausgeber, zum Druck im Oldenbourg-Verlag angenommen wurden und im nächsten Jahr erscheinen werden. Das eine dieser zwei Bücher trägt den Titel „Zahlentheorie“, hat zweihundert Seiten und zeugt davon, wie nachhaltig sich Heinz Lüneburg mit der Entwicklung der Zahlentheorie beschäftigt hat. Mit den drei Büchern von Euklid startend, die die zahlentheoretischen heißen, gelangt er zu den Ringen der ganzen algebraischen Zahlen und dem fermatschen Zwei–Quadrate–Satz. Im zweiten 220 Seiten umfassenden Buch mit dem Titel „Größen und Zahlen. Ein Aufbau des Zahlensystems auf der Grundlage der eudoxischen Proportionenlehre“ lässt er von seinem früheren Vervollständigen der rationalen Zahlen durch Cauchyfolgen ab und wendet sich den dedekindschen Schnitten auf der Menge der positiven rationalen Zahlen zu, wobei er anschließend die negativen reellen Zahlen auf die gleiche Weise gewinnt, wie man die negativen ganzen Zahlen aus den natürlichen bekommt. So erhält er gleichzeitig mit den reellen Zahlen alle Logarithmus- sowie alle Exponentialfunktionen.

Das dritte hinterlassene Werk ist ein 108-seitiges Manuskript „Streifzüge durch die Geschichte der Mathematik“, das besonders reizvoll ist, weil Heinz Lüneburg darin in lockerer Form die im Laufe seines Lebens gewonnenen geschichtlichen Erkenntnisse über Zahlen versammelt, Erkenntnisse von den natürlichen bis zu den rationalen Zahlen. Ich persönlich bin am meisten von dem in dem Buch vorgesehen Vokabular gefesselt, in welchem Heinz Lüneburg vorhatte, die Herkunft der von den Mathematikern meistbenutzten Wörter bloßzulegen, denn das meiste war für mich überraschend und neu und zeigte mir meinen Mangel an klassischer Bildung. Die Lektüre dieses Vokabulars ist sehr vergnüglich, was hier an dem Wort Korollar erläutert sei: Das lateinische Corollarium ist das Kränzchen, das der Gastgeber seinen Zechkumpanen aufs Haupt drückt, wenn sie zum Symposion (griechisch für Gelage) kommen. Leider ist dieses Manuskript nicht ganz vollständig.

Heinz Lüneburg war ein Freund, auf den man sich verlassen konnte. Er hat mit seinen Meinungen nie hinterm Berg gehalten und sich seine Gradlinigkeit ein Leben lang bewahrt. Seine Mathematik bleibt in uns gut aufgehoben, so lange wir leben. Die Lüneburgebenen bleiben aktuell, so lange man sich für projektive Ebenen und Suzuki–Gruppen interessiert. Dass er sich aus dem Kraal der Mathematiker hinausgewagt hat, wird sich für sein Gedenken in der Zukunft lohnen. Während die wenigen kompetenten Bücher fürs breite Publikum, die die Mathematik aus der Geschichte herauswachsen lassen, naive, unmittelbare Begeisterung entfachen und sich jahrzehntelang eines Zu-

spruchs erfreuen können, muss ein mathematischer Aufsatz außerhalb des engsten Spezialistenkreises um die Aufmerksamkeit der in Anbetracht der Flut der Veröffentlichungen abgebrühten Mathematikergilde hart und manchmal ohne Erfolg kämpfen.

Literatur

Johannes André, *Über nicht-Desarguessche Ebenen mit transitiver Translationsgruppe.* Math. Z. 60, 156–186, 1954

Emil Artin, *Geometric Algebra.* New York, London 1957

Reinhold Baer, *Homogeneity of projective planes.* Amer. J. Math. 64, 137–152, 1942
— *Polarities of finite projective planes.* Bull. Amer. Math. Soc. 53, 77–93, 1946a
— *Projectivities with fixed points on every line of the plane.* Bull. Amer. Math. Soc. 52, 273– 286, 1946b
— *Linear Algebra and Projective Geometry.* New York 1952 (Struktursätze)

Richard Brauer, *A Characterization of Null Systems in Projective Space.* Bull. Amer. Math. Soc. 42, 247–254, 1936 (Beweist u. A., dass jede Kollineation von einer semilinearen Abbildung induziert wird; vorausgesetzt wird jedoch, dass der Körper kommutativ ist. Benutzt Doppelverhältnisse. Der Satz sei bekannt, sein Beweis jedoch kürzer.)
— *On the connection between the ordinary and the modular characters of groups of finite order.* Ann. Math. 42, 926–935, 1941 (Satz IIII.3.4)

Egbert Brieskorn und Horst Knörrer, *Algebraische Kurven.* Math. Institut Bonn, o. J. (Birkhäuser 1981)

Richard H. Bruck and Herbert J. Ryser, *The non-existence of certain finite projective planes.* Canadian J. Math. 1, 88–93, 1949

W. L. Chow, *On the Geometry of Algebraic Homogeneous Spaces.* Ann. Math. 50, 32–67, 1949 (Satz von Chow für beliebige irreduzible projektive Räume, aber $r = s$.)

Paul M. Cohn, *Skew field constructions.* Cambridge 1977
(Körper mit $(K^*)' = K^*$.)

Richard Dedekind, *Über Zerlegungen von Zahlen durch ihre größten gemeinsamen Teiler.* Festschrift der TH Braunschweig. 1–40, 1897. Werke, Band 2, 103–147, 1931

Peter Dembowski, *Verallgemeinerungen von Transitivitätsklassen endlicher projektiver Ebenen.* Math. Z. 69, 59–89, 1958
— *Finite Geometries.* Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 44. Berlin, etc. 1968

Ulrich Dempwolff, *Über die Determinante.* Math. Semesterberichte 40, 193–197, 1993

Max Deuring, *Algebren.* Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 41. 2. Auflage. Berlin, Heidelberg, New York 1968

Leonard Eugene Dickson, *Linear Groups with an Exposition of the Galois Field Theory.* Nachdruck der ersten Auflage. New York 1958. In dieser Auflage ist das Vorwort zur ersten Auflage mit November 1900 datiert.

Jean Dieudonné, *Les déterminants sur un corps non commutatif.* Bull. Soc. Math. France 71, 27–45, 1943 (Zitiert nach Dieudonné 1955)
— *La géométrie des groupes classiques.* Ergebnisse der Mathematik und ihrer Grenzgebiete. Neue Folge Band 5. Berlin, etc. 1955

R. A. Fisher, *An examination of the different possible solutions of a problem in incomplete blocks.* Ann. of Eugenics 10, 52–75, 1940 (Zitiert nach Dembowski 1968. Fisher'sche Ungleichung.)

G. Frobenius, *Über lineare Substitutionen und bilineare Formen.* J. reine angew. Math. 84, 1–63, 1877

Carl Friedrich Gauß, *Demonstration nova altera theorematis omnem functionem algebraicam rationalem integram unius variabilis in factores reales primi vel secundi gradus resolvi posse.* Comm. soc. reg. sci. Gottingensis. rec. III. Göttingen 1816. Werke, Band 3, 31–56, 1876

William Rowan Hamilton, *Memorandum respecting a new system of roots of unity.* Phil. Mag. (4), 12, 446, 1856 (Satz III.4.5: Präsentation von A_5.)

I. N. Herstein, *Noncommutative Rings.* The Carus Mathematical Monographs 15. Published by The Mathematical Association of America. Kein Ort. 1968

Armin Herzer, *Dualitäten mit zwei Geraden aus absoluten Punkten in projektiven Ebenen.* Math. Z. 129, 235–257, 1972

Otto Hesse, *Über die Elimination der Variabeln aus drei algebraischen Gleichungen vom zweiten Grade mit zwei Variabeln.* J. reine angew. Mathematik 28, 68–96, 1844
— *Algebraische Auflösung derjenigen Gleichungen 9ten Grades, deren Wurzeln die Eigenschaft haben, dass eine gegebene rationale und symmetrische Function $\theta(x_\lambda, x_\mu)$ je zweier Wurzeln x_λ, x_μ eine dritte Wurzel x_κ giebt, so dass gleichzeitig: $x_\kappa = \theta(x_\lambda, x_\mu)$, $x_\lambda = \theta(x_\mu, x_\kappa)$, $x_\mu = \theta(x_\kappa, x_\lambda)$.* J. reine angew. Mathematik 34, 193–208, 1847

Gerhard Hessenberg, *Beweis des Desarguesschen Satzes aus dem Pascalschen.* Math. Ann. 61, 161–172, 1905

David Hilbert, *Grundlagen der Geometrie.* Leipzig 1899

Otto Hölder, *Die einfachen Gruppen im ersten und zweiten Hundert der Ordnungszahlen.* Math. Ann. 40, 55–88, 1892

Daniel R. Hughes und Fred C. Piper, *Projective Planes.* New York, etc. 1973

Bertram Huppert, *Endliche Gruppen I.* Berlin, etc. 1973

K. Iwasawa, *Über die Einfachheit der speziellen projektiven Gruppe.* Proc. Imp. Acad. Tokyo 17, 57–59, 1962 (Zitiert nach Huppert 1973)

John Jackson, *Rational Amusements for Winter Evenings.* London 1821

Camille Jordan, *Traité des substitutions et des équations algébriques.* Nachdruck der Ausgabe Paris 1870. Sceaux 1989

Helmut Karzel, *Zweiseitige Inzidenzgruppen.* Abh. Math. Sem. Univ. Hamburg 29, 118–136, 1965

Heinz Lüneburg, *Ein neuer Beweis eines Hauptsatzes der projektiven Geometrie.* Math. Z. 87, 32–36. 1965
— *Über die Struktursätze der projektiven Geometrie.* Arch. Math. 17, 206–209, 1966
— *Einige methodische Bemerkungen zur Theorie der elliptischen Bewegungsgruppen.* Abh. Math. Sem. Univ. Hamburg 34, 59–72, 1969a
— *Lectures on projective planes.* Notes prepared by Mark Pankin and William Patton. Lectures given during 1968/69 at the University of Illinois at Chicago Circle. Dept. of Mathematics, University of Illinois at Chicago Circle 1969b
— *Einführung in die Algebra.* Berlin, etc. 1973
— *Translation Planes.* Berlin, Heidelberg, New York 1980
— *Tools and Fundamental Constructions of Combinatorial Mathematics.* Mannheim 1989

Fumitomo Maeda, *Kontinuierliche Geometrien.* Berlin, Göttingen, Heidelberg 1958

Helmut Mäurer, *Zur Automorphismengruppe der symmetrischen Gruppe.* Mitt. Math. Ges. Hamburg XI, 265–266, 1983

Eliakim Hastings Moore, *Concerning the abstract Group of order $k!$ and $\frac{1}{2}k!$.* Proc. London Math. Soc. (1), 28, 357–366, 1897
— *Concerning the general equation of the seventh and eighth degrees.* Math. Ann. 51, 417–444, 1899

P. J. Morandi, B. A. Sethuraman und J.-P. Tignol, *Division algebras with an anti-automorphism but with no involution.* Adv. Geom. 5, 485–495, 2005

Eugen Netto, *Substitutionentheorie und ihre Anwendungen auf die Algebra.* Leipzig 1882

Peter Neumann, *A Lemma that is not Burnside's.* The Mathematical Scientist 4, 133–141, 1979 (Sätze IIII.1.6 und IIII.1.7.)

John von Neumann, *Continuous Geometry.* Princeton, London 1960

Theodore Ostrom und Ascher Wagner, *On projective and affine planes with transitive collineation groups.* Math. Z. 71, 186–199, 1959

Günter Pickert, *Projektive Ebenen.* Berlin, Göttingen, Heidelberg 1955 (Zweite Auflage 1975)

A. Rosenberg, *The Structure of the Infinite General Linear Group.* Ann. Math. 68, 278–297, 1958

G. Salmon, *Lettre de Mr. G. Salmon de Dublin à l'éditeur de ce journal.* J. reine angew. Math. 39, 365–366, 1850

Issai Schur, *Neue Begründung der Theorie der Gruppencharaktere.* Sitzungsberichte der Preussischen Akademie der Wissenschaften 1905, Phys.-Math. Klasse, 406–432. Werke Band 1, 143–169

Helga Tecklenburg, *A Proof of the Theorem of Pappos in Finite Desarguesian Affine Planes.* J. Geom. 30, 172–181, 1987

O. Veblen und J. W. Young, *Projective Geometry.* 2. Auflage. Band I, Boston 1916. Band II, Boston 1917

Ascher Wagner, *A theorem on doubly transitive permutation groups.* Math. Z. 85, 451–453, 1964 (Sätze IIII.8.4, IIII.8.5, IIII.8.6.)
— *On finite affine line transitive planes.* Math. Z. 87, 1–11, 1965 (Geradenhomogene affine Ebenen sind Translationsebenen. Dieser Satz wurde in Ostrom und Wagner 1959 vermutet. Satz IIII.9.11.)

Helmut Wielandt, *Unendliche Permutationsgruppen.* Vorlesungen an der Univ. Tübingen 1959/60 (Englische Übersetzung in: Mathematische Werke vol. 1. De Gruyter, Berlin 1994).

Max Zorn, *Theorie der alternativen Ringe.* Abh. Math. Sem. Univ. Hamburg 8, 123–147, 1931 (Hierin der Satz IIII.6.14 und der Satz von Artin-Zorn. Beide Sätze stammen laut Zorn von E. Artin.)

Index